DISPOSITIVOS DE RED Y CONFIGURACION INICIAL CISCO

Contenido

Módulo 1: Diseño de redes 7
0. Introducción 7
1.0.1 Primera Vez en Este Curso 7
1.0.2 Recursos del Estudiante 7
1.0.3 Webster - ¿Por Qué Debería Tomar este Módulo? 7
1.0.4 ¿Qué Aprenderé en este Módulo? 7
1. Redes Confiables 8
1.1.1 Arquitectura de la Red 8
1.1.2 Vídeo - Tolerancia a Fallas 8
1.1.3 Tolerancia a Fallas 9
1.1.4 Escalabilidad 9
1.1.5 Calidad de Servicio 9
1.1.6 Seguridad de la Red 10
1.1.7 Verifique su Comprensión - Redes Confiables 10
2. Diseño Jerárquico de Redes 10
1.2.1 Direcciones Físicas y Lógicas 10
1.2.2 Video - Ver Información de Red en Mi Dispositivo 11
1.2.3 Laboratorio - Ver la información de una NIC Inalámbrica y Cableada 11
1.2.4 Analogía Jerárquica 13
1.2.5 Video - Beneficios de un Diseño de Redes Jerárquico 13
1.2.6 Acceso, Distribución y Núcleo 14
1.2.7 Verifique su Comprensión - Diseño de Redes Jerárquico 14
3. Resumen de diseño de redes 14
1.3.1 ¿Qué Aprendí en este Módulo? 14
1.3.2 Webster - Preguntas de Reflexión 15
1.3.3 Prueba de Diseño de Redes 15
Módulo 2: La Nube y Virtualización 16
0. Introducción 16
2.0.1 Webster - ¿Por Qué Debería Tomar este Módulo? 16
2.0.2 - ¿Qué Aprenderé en este Módulo? 16
1. La nube y servicios en la nube 16
2.1.1 Vídeo - La Nube y Virtualización 16
2.1.2 Tipos de Nubes 17
2.1.3 Computación en la Nube y Virtualización 17
2.1.4 Verifique su comprensión - La Nube y Servicios en la Nube 18
2. Virtualización 18
2.2.1 Ventajas de la Virtualización 18
2.2.2 Hipervisores 18
2.2.3 Laboratorio - Instalar de Linux en una Máquina Virtual y Explorar la GUI 19
3. Resumen de la nube y virtualización 21
2.3.1 ¿Qué Aprendí en este Módulo? 21
2.3.2 Webster - Preguntas de Reflexión 22
2.3.3 Prueba de La Nube y Virtualización 22
Módulo 3: Sistemas de Numeración 23
0. Introducción 23
3.0.1 Webster - ¿Por Qué Debería Tomar este Módulo? 23
3.0.2 ¿Qué Aprenderé en este Módulo? 23
1. Sistema numérico binario 23
3.1.1 Direcciones Binarias e IPv4 23
3.1.2 Video - Conversión Entre Sistemas de Numeración Binarios y Decimales 23
3.1.3 Verifique su Comprensión - Sistema Numérico Binario 24
3.1.4 Actividad - Conversión de Binario a Decimal 24
3.1.5 Conversión de Decimal a Binario 25
3.1.6 Ejemplo de Conversión de Decimal a Binario 26

3.1.7 Actividad - Conversión de Decimal a Binario ... 26
3.1.8 Actividad - Juego Binario ... 26
3.1.9 Direcciones IPv4 ... 26
2. Sistema numérico hexadecimal ... 27
3.2.1 Direcciones Hexadecimales e IPv6 ... 27
3.2.2 Vídeo - Conversión Entre Sistemas de Numeración Hexadecimal y Decimal ... 28
3.2.3 Verifique su Comprensión - Convierta entre Sistemas Numéricos Decimales a Hexadecimales ... 28
3. Resumen de sistemas numéricos ... 29
3.3.1 ¿Qué Aprendí en este Módulo? ... 29
3.3.2 Webster - Preguntas de Reflexión ... 29
3.3.3 Prueba de Sistemas Numéricos ... 29
Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 1 – 3 ... 29
Módulo 4: Conmutación Ethernet ... 31
0. Introducción ... 31
4.0.1 Webster - ¿Por Qué Debería Tomar este Módulo? ... 31
4.0.2 ¿Qué Aprenderé en este Módulo? ... 31
1. Ethernet ... 32
4.1.1 El Auge de Ethernet ... 32
4.1.2 Evolución de Ethernet ... 32
4.1.3 Vídeo - Direccionamiento Ethernet ... 32
4.1.4 Laboratorio - Determinar la Dirección MAC de un Host ... 33
2. tramas de Ethernet ... 34
4.2.1 Encapsulación de Ethernet ... 34
4.2.2 Subcapas de la capa Enlace de Datos ... 34
4.2.3 La Subcapa MAC ... 34
4.2.4 Campos de la Trama de Ethernet ... 35
4.2.5 Verifique su Comprensión - La Trama Ethernet ... 36
4.2.6 Laboratorio - Visualización del Tráfico Capturado en Wireshark ... 36
4.2.7 Laboratorio - Uso de Wireshark para Examinar Tramas Ethernet ... 40
3. Dirección MAC de Ethernet ... 43
4.3.1 Dirección MAC y Hexadecimal ... 43
4.3.2 Dirección MAC de Unidifusión (Unicast) ... 44
4.3.3 Dirección MAC de Difusión (Broadcast) ... 44
4.3.4 Dirección MAC de Multidifusión (Multicast) ... 45
4.3.5 Verifique su Comprensión - Dirección MAC Ethernet ... 46
4. La Tabla de direcciones MAC ... 46
4.4.1 Fundamentos del Conmutador ... 46
4.4.2 Aprendizaje y Reenvío del Conmutador ... 46
4.4.3 Filtrado de Tramas ... 47
4.4.4 Video - Tablas de Direcciones MAC en Conmutadores Conectados ... 48
4.4.5 Video - Envío de la Trama a la Puerta de Enlace Predeterminada ... 49
4.4.6 Actividad – Conmútelo ... 49
5. Resumen de conmutación Ethernet ... 50
4.5.1 ¿Qué Aprendí en este Módulo? ... 50
4.5.2 Webster – Reflexión ... 51
4.5.3 Prueba de Conmutación Ethernet ... 51
Módulo 5: La Capa de Red ... 52
0. Introducción ... 52
5.0.1 Webster ... 52
5.0.2 ¿Qué Voy a Aprender en este Módulo? ... 52
1. Características de la Capa de Red ... 52
5.1.1 Vídeo - Encapsulación de Datos ... 52
5.1.2 La Capa de Red ... 53
5.1.3 Encapsulación IP ... 53
5.1.4 Características de IP ... 54

5.1.5 Sin Conexión 54
5.1.6 Mejor Esfuerzo 54
5.1.7 Independiente de los Medios 55
5.1.8 Verifique su Comprensión - Características de IP 55
2. Paquete IPv4 55
5.2.1 Encabezado del Paquete IPV4 55
5.2.2 Campos del Encabezado del Paquete IPV4 55
5.2.3 Video - Ejemplos del Encabezado de IPV4 en Wireshark 56
5.2.4 Verifique su Comprensión - Paquete IPv4 56
3. Paquete IPv6 57
5.3.1 Limitaciones de IPv4 57
5.3.2 Descripción General de IPv6 57
5.3.3 Campos del Encabezado del Paquete IPv4 en el Encabezado del Paquete IPv6 57
5.3.4 Encabezado del Paquete IPv6 58
5.3.5 Video - Ejemplos del Encabezado IPV6 en Wireshark 58
5.3.6 Verifique su Comprensión - Paquete IPv6 59
4. Resumen de la Capa de Red 60
5.4.1 ¿Qué Aprendí en este Módulo? 60
5.4.2 Webster - Preguntas de Reflexión 60
5.4.3 Prueba de la Capa de Red 60
Módulo 6: Direccionamiento IPv4 61
0. Introducción 61
6.0.1 Webster - ¿Por qué debería tomar este módulo? 61
6.0.2 ¿Qué Voy a Aprender en este Módulo? 61
1. Estructura de la dirección IPv4 61
6.1.1 Porciones de Red y de Host 61
6.1.2 La Máscara de Subred 62
6.1.3 La Longitud del Prefijo 62
6.1.4 Determinación de la Red: AND lógico 62
6.1.5 Video - Direcciones de Red, Host y Difusión. 63
6.1.6 Actividad - Uso del AND para Determinar la Dirección de Red 64
6.1.7 Verifique su Comprensión - Estructura de la Dirección IPv4 64
2. Resumen de direccionamiento IPv4 65
6.2.1 ¿Qué Aprendí en este Módulo? 65
6.2.2 Webster - Preguntas de Reflexión 65
6.2.3 Prueba de Direccionamiento IPv4 65
Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 4 – 6 66
Módulo 7: Resolución de dirección 69
0. Introducción 69
7.0.1 Webster - ¿Por Qué Debería Tomar este Módulo? 69
7.0.2 ¿Qué Voy a Aprender en este Módulo? 69
1. ARP 69
7.1.1 Descripción General de ARP 69
7.1.2 Funciones de ARP 70
7.1.3 Video - Operación de ARP - Solicitud de ARP 70
7.1.4 Vídeo - Operación de ARP - Respuesta de ARP 71
7.1.5 Video - El Rol de ARP en Comunicaciones Remotas 71
7.1.6 Eliminando Entradas de una Tabla de ARP 72
7.1.7 Tablas de ARP en Dispositivos 72
7.1.8 Problemas de ARP - Difusiones de ARP y Suplantación de Identidad de ARP 73
7.1.9 Packet Tracer - Examinar la Tabla de ARP 73
7.1.10 Laboratorio - Ver Tráfico ARP en Wireshark 75
7.1.11 Verifique su Comprensión – ARP 78
2. Resumen de Resolución de Direcciones 78
7.2.1 ¿Qué Aprendí en este Módulo? 78

7.2.2 Webster - Preguntas de Reflexión ... 79
7.2.3 Prueba de Resolución de Direcciones ... 79
Módulo 8: Servicios de Direccionamiento IP ... 80
0. Introducción ... 80
8.0.1 Webster - ¿Por Qué Debería Tomar este Módulo? ... 80
8.0.2 ¿Qué Aprenderé en este Módulo? ... 80
1. Servicios de DNS ... 80
8.1.1 Vídeo - Sistema de Nombres de Dominio ... 80
8.1.2 Sistema de Nombres de Dominio ... 81
8.1.3 Formato de Mensajes DNS ... 82
8.1.4 La Jerarquía DNS ... 82
8.1.5 El Comando nslookup ... 83
8.1.6 Comprobador de Sintaxis — El Comando nslookup ... 83
8.1.7 Verifique su Comprensión - Servicios de DNS ... 84
8.1.8 Laboratorio - Observar la Resolución de DNS ... 84
2. Servicios de DHCP ... 87
8.2.1 Protocolo de Configuración Dinámica de Host ... 87
8.2.2 Vídeo - Funcionamiento de DHCP en un Enrutador Doméstico ... 88
8.2.3 Mensajes DHCP ... 88
8.2.4 Verifique su Comprensión - Servicios de DHCP ... 89
3. Resumen de Servicios de Direccionamiento IP ... 89
8.3.1 ¿Qué Aprendí en este Módulo? ... 89
8.3.2 Webster - Preguntas de Reflexión ... 90
8.3.3 Prueba de Servicios de Direccionamiento IP ... 90
Módulo 9: La Capa de Transporte ... 91
0. Introducción ... 91
9.0.1 Webster - ¿Por Qué Debería Tomar este Módulo? ... 91
9.0.2 ¿Qué Voy a Aprender en este Módulo? ... 91
1. Transporte de datos ... 92
9.1.1 Función de la Capa de Transporte ... 92
9.1.2 Tareas de la capa Transporte ... 92
9.1.3 Protocolos de la capa Transporte ... 94
9.1.4 Protocolo de Control de Transmisión (TCP) ... 94
9.1.5 Protocolo Datagramas de Usuario (UDP) ... 95
9.1.6 El Protocolo de capa Transporte adecuado para la aplicación adecuada ... 96
9.1.7 Verifique su Comprensión - Transporte de Datos ... 96
2. Descripción general de TCP ... 97
9.2.1 Características de TCP ... 97
9.2.2 El Encabezado TCP ... 97
9.2.3 Campos del Encabezado TCP ... 97
9.2.4 Aplicaciones que Utilizan TCP ... 97
9.2.5 Verifique su Comprensión - Descripción General de TCP ... 98
3. Descripción general de UDP ... 98
9.3.1 Características de UDP ... 98
9.3.2 El Encabezado UDP ... 98
9.3.3 Campos del Encabezado UDP ... 98
9.3.4 Aplicaciones que Utilizan UDP ... 99
9.3.5 Verifique su Comprensión - Descripción General de UDP ... 99
4. Números de Puerto ... 99
9.4.1 Comunicaciones Separadas Múltiples ... 99
9.4.2 Pares de Sockets ... 100
9.4.3 Grupos de Números de Puerto ... 100
9.4.4 El Comando netstat ... 101
9.4.5 Verifique su Comprensión - Números de Puerto ... 101
5. Proceso de Comunicación TCP ... 101

9.5.1 Procesos del Servidor TCP 101
9.5.2 Establecimiento de Conexiones TCP 103
9.5.3 Terminación de la Sesión 104
9.5.4 Análisis del Protocolo TCP de Enlace de Tres Vías 105
9.5.5 Video - Protocolo TCP de Enlace de 3 Vías 106
9.5.6 Verifique su Comprensión - Proceso de Comunicación TCP 107
6. Confiabilidad y Control de Flujo 107
9.6.1 Confiabilidad de TCP - Entrega Garantizada y Ordenada 107
9.6.2 Video - Confiabilidad de TCP - Números de Secuencia y Acuses de Recibo 108
9.6.3 Confiabilidad de TCP - Pérdida de Datos y Retransmisión 109
9.6.4 Vídeo - Confiabilidad TCP - Pérdida de Datos y Retransmisión 110
9.6.5 Control de Flujo TCP - Tamaño de la Ventana y Acuses de Recibo 111
9.6.6 Control de Flujo TCP - Tamaño Máximo de Segmento (MSS) 112
9.6.7 Control de Flujo TCP - Prevención de Congestión 112
9.6.8 Verifique su Comprensión - Confiabilidad y Control de Flujo 113
7. Comunicación UDP 113
9.7.1 Bajo Costo UDP versus Confiabilidad 113
9.7.2 Rearmado de Datagramas UDP 113
9.7.3 Procesos y Solicitudes del Servidor UDP 113
9.7.4 Procesos de Cliente UDP 114
9.7.5 Verifique su Comprensión - Comunicación UDP 115
8. Resumen de la Capa de Transporte 116
9.8.1 Packet Tracer - Comunicaciones TCP y UDP 116
9.8.2 ¿Qué Aprendí en este Módulo? 118
9.8.3 Webster - Preguntas de Reflexión 121
9.8.4 Prueba de La Capa de Transporte 121
Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 7 – 9 122
Modulo 10: La Línea de Comandos del IOS de Cisco 125
0. Introducción 125
10.0.1 Webster - ¿Por Qué Debería Tomar este Módulo? 125
10.0.2 ¿Qué Voy a Aprender en este Módulo? 125
1. Navegación del IOS 125
10.1.1 La Interfaz de Línea de Comandos del IOS de Cisco 125
10.1.2 Modos de Comando Principales 126
10.1.3 Video - Modos de Comando Principales de la CLI del IOS 126
10.1.4 Video - Navegando Entre los Modos del IOS 127
10.1.5 Una Nota Sobre las Actividades del Verificador de Sintaxis 127
10.1.6 Verificador de Sintaxis - Navegar entre los Modos IOS 127
10.1.7 Verifique su Comprensión - Navegación del IOS 127
2. La estructura de comandos 128
10.2.1 Estructura Básica de los Comandos de IOS 128
10.2.2 Sintaxis de los Comandos de IOS 128
10.2.3 Video - Ayuda Sensible al Contexto y Verificación de Sintaxis de Comandos 129
10.2.4 Teclas de Acceso Rápido y de Método Abreviado 129
10.2.5 Video - Teclas de Acceso Rápido y Métodos Abreviados 130
10.2.6 Packet Tracer - Navegar por el IOS 131
3. Ver la información del dispositivo 133
10.3.1 Video - Comandos Show del IOS de Cisco 133
10.3.2 Comandos Show 133
10.3.3 Packet Tracer - Uso de los Comandos Show del IOS de Cisco 137
4. Resumen de la línea de comandos del IOS de Cisco 138
10.4.1 ¿Qué Aprendí en este Módulo? 138
10.4.2 Webster - Preguntas de Reflexión 138
10.4.3 Prueba de La Línea de Comandos del IOS de Cisco 138
Módulo 11: Crear una Pequeña Red de Cisco 139

0. Introducción 139
11.0.1 Webster - ¿Por Qué Debería Tomar este Módulo? 139
11.0.2 ¿Qué Aprenderé en este Módulo? 140
1. Configuración básica del Conmutador 140
11.1.1 Pasos Básicos en la Configuración de un Conmutador 140
11.1.2 Configuración de la Interfaz Virtual del Conmutador (SVI) 141
11.1.3 Verificador de Sintaxis - Configuración de una Interfaz Virtual del Conmutador 141
11.1.4 Packet Tracer - Implementar la Conectividad Básica 141
2. Configurar los ajustes iniciales del enrutador 143
11.2.1 Pasos Básicos de Configuración del Enrutador 143
11.2.2 Ejemplo de Configuración Básica del Enrutador 143
11.2.3 Verificador de Sintaxis - Configurar los Ajustes Iniciales del Enrutador 144
11.2.4 Packet Tracer: Configurar los Parámetros Iniciales del Enrutador 145
3. Asegurar los dispositivos 147
11.3.1 Recomendaciones para Contraseñas 147
11.3.3 Habilitar SSH 148
11.3.4 Verificador de Sintaxis - Configuración de SSH 149
11.3.5 Verificar SSH 149
11.3.6 Packet Tracer - Configurar SSH 150
4. Configuración de la puerta de enlace predeterminada 152
11.4.1 Puerta de Enlace Predeterminada en un Host 152
11.4.2 Puerta de Enlace Predeterminada en un Conmutador 153
11.4.3 Verificador de Sintaxis — Configurar la Puerta de Enlace Predeterminada 153
11.4.4 Actividad Guiada de Packet Tracer - Crear una Red con un Conmutador y un Enrutador 153
11.4.5 Packet Tracer - Solución de Problemas de la Puerta de Enlace Predeterminada 158
5. Resumen de crear una pequeña red de Cisco 160
11.5.1 ¿Qué Aprendí en este Módulo? 160
11.5.2 Webster - Preguntas de Reflexión 161
11.5.3 Prueba de Crear una Pequeña Red de Cisco 161
Módulo 12: ICMP Protocolos de Mensajes de Control de Internet 162
0. Introducción 162
12.0.1 Webster: ¿Por Qué Debería Tomar este Módulo? 162
12.0.2 ¿Qué Aprenderé en este Módulo? 162
1. Mensajes ICMP 162
12.1.1 Mensajes ICMPv4 e ICMPv6 162
12.1.2 Accesibilidad del Host 162
12.1.3 Destino o Servicio Inalcanzable 163
12.1.4 Tiempo Excedido 163
12.1.5 Mensajes ICMPv6 163
12.1.6 Verifique su Comprensión - Mensajes ICMP 165
2. Pruebas de ping y traceroute 165
12.2.1 Ping - Probar la Conectividad 165
12.2.2 Hacer Ping al Loopback 165
12.2.3 Hacer Ping a la Puerta de Enlace Predeterminada 166
12.2.5 Traceroute - Probar el Camino 167
12.2.6 Packet Tracer - Verificar el Direccionamiento IPv4 e IPv6 168
12.2.7 Packet Tracer - Usar Ping y Traceroute para Probar la Conectividad de Red 169
3. Resumen de ICMP 171
12.3.1 Packet Tracer - Utilizar ICMP para Probar y Corregir la Conectividad de Red 171
12.3.2 ¿Qué Aprendí en este Módulo? 172
12.3.3 Webster - Preguntas de Reflexión 173
12.3.4 Prueba de ICMP 173
Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 10 – 12 174
Examen Final de Dispositivos de Red y Configuración Inicial 177

Módulo 1: Diseño de redes

0. Introducción

1.0.1 Primera Vez en Este Curso

Este curso enseña conocimientos y destrezas intermedios para redes, cubriendo los conceptos básicos y las destrezas necesarias para construir una red de oficina en el hogar y una pequeña red de oficina de Cisco. Al alumno se le presenta una vista atractiva y exploratoria de las redes, los dispositivos que las componen, cómo funcionan y las herramientas y técnicas para solucionar problemas. Prepara al alumno para pasar a la ciberseguridad o DevNet profundizando en Ethernet, el direccionamiento IP y la capa de transporte. También cubre la configuración de dispositivos de Cisco y finaliza con la capacidad de configurar y solucionar problemas en una pequeña red de Cisco. El objetivo de este curso es proporcionar al alumno una descripción general intermedia del diseño, la estructura y las operaciones de la red. Al finalizar el curso de Dispositivos de Red y Configuración Inicial, los estudiantes podrán realizar las siguientes tareas:

- Explicar los componentes de un diseño de redes jerárquico.
- Explicar las características de la virtualización y los servicios en la nube.
- Calcular números entre los sistemas decimales, binarios y hexadecimales.
- Explicar cómo funciona Ethernet en una red conmutada.
- Explicar cómo los enrutadores utilizan los protocolos y los servicios de capa de red para habilitar la conectividad integral.
- Calcular un esquema de subredes IPv4 para segmentar la red de manera eficiente.
- Explicar cómo ARP permite la comunicación en una red de área local.
- Explicar cómo funcionan los servicios DNS y DHCP.
- Comparar el funcionamiento de los protocolos de capa de transporte en la admisión de la comunicación de extremo a extremo.
- Usar el IOS de Cisco.
- Armar una red de computadoras simple con dispositivos Cisco.
- Utilizar varias herramientas para probar la conectividad de red.

1.0.2 Recursos del Estudiante

Hay una serie de herramientas y recursos disponibles para usted que lo ayudarán en su viaje a medida que desarrolla sus habilidades para establecer contactos y se prepara para las oportunidades laborales.

Packet Tracer

Packet Tracer simula el funcionamiento interno de una red y se utiliza en este curso. Si es nuevo en Packet Tracer, tome este breve curso en línea gratuito: ***Introducción a Cisco Packet Tracer***. Puede hacer uso de su teléfono móvil inteligente, tableta o PC para acceder al curso; sin embargo, para las actividades de Packet Tracer, así como también para otras actividades, pruebas y exámenes, obtendrá una mejor experiencia si usa una computadora.

Entorno de laboratorio

No se necesitan equipos

Recursos disponibles para usted

Las preguntas frecuentes sobre Skills for All se pueden encontrar en https://skillsforall.com/help o haciendo clic en Help en la barra de navegación superior. Para obtener ayuda con la descarga de Packet Tracer, visite https://skillsforall.com/resources/lab-downloads y desplácese hacia abajo hasta Recursos de aprendizaje (Learning Resources).

Puede encontrar preguntas frecuentes adicionales visitando nuestro asistente virtual, Morgan. Haga clic en el ícono de chat en la esquina superior derecha para elegir entre una lista de temas o ingresar tu pregunta. La ayuda de Morgan incluye información sobre Packet Tracer, certificados e insignias.

1.0.3 Webster - ¿Por Qué Debería Tomar este Módulo?

¡Bienvenido a Dispositivos de Red y Configuración Inicial! Soy Webster y me verán durante todo el curso. ¡Permítame presentarle a mi amigo Bob! Bob trabaja en el campo de TI en Vancouver, Canadá, y tiene experiencia en redes. Está asesorando a sus amigos, Marcy y Vincent, quienes han comprado una mueblería. Quieren expandir sus operaciones físicas y establecerse en la tienda en línea. Actualmente, la red interna de la tienda maneja el inventario y las transacciones en la tienda. Marcy y Vincent desean agregar cámaras de seguridad, teléfonos VoIP y también expandirla para incluir el comercio electrónico y el envío de los productos. Bob explica que esto será más costoso de lo que sus amigos habían previsto. Está pensando en diseñar la red futura para la mueblería. Explica que debe tener en cuenta la tolerancia a fallas, la escalabilidad, la QoS y la seguridad. Además, su red es actualmente plana, no jerárquica. Las redes jerárquicas escalan bien y se adaptan mejor a este negocio en crecimiento.

¡Vaya! Eso es mucho para que Marcy y Vincent lo entiendan. No están familiarizados con estos problemas de red. ¿Y usted? ¡Tome este módulo para obtener más información sobre redes confiables y diseño de redes jerárquico!

1.0.4 ¿Qué Aprenderé en este Módulo?

Título del módulo: Diseño de Redes

Objetivo del Módulo: Explicar los componentes de un diseño de redes jerárquico.

Título del Tema	Objetivo del Tema
Redes Confiables	Describa los cuatro requisitos básicos de una red confiable.
Diseño de Redes Jerárquico	Explique la función en cada capa del modelo de diseño de red de 3 capas.

1. Redes Confiables

1.1.1 Arquitectura de la Red

¿Alguna vez ha estado ocupado trabajando en línea, y " se cayó Internet "? Como ya sabe, Internet no se cayó, simplemente perdió la conexión. Es muy frustrante. Con tantas personas en el mundo que dependen del acceso a la red para trabajar y aprender, es imperativo que las redes sean confiables. En este contexto, la fiabilidad significa más que su conexión a Internet. Este tema se centra en los cuatro aspectos de la fiabilidad de la red.

La función de la red cambió de una red únicamente de datos a un sistema que permite conectar personas, dispositivos e información en un entorno de red convergente y con gran variedad de medios. Para que las redes funcionen eficazmente y crezcan en este tipo de entorno, se deben crear sobre la base de una arquitectura de red estándar.

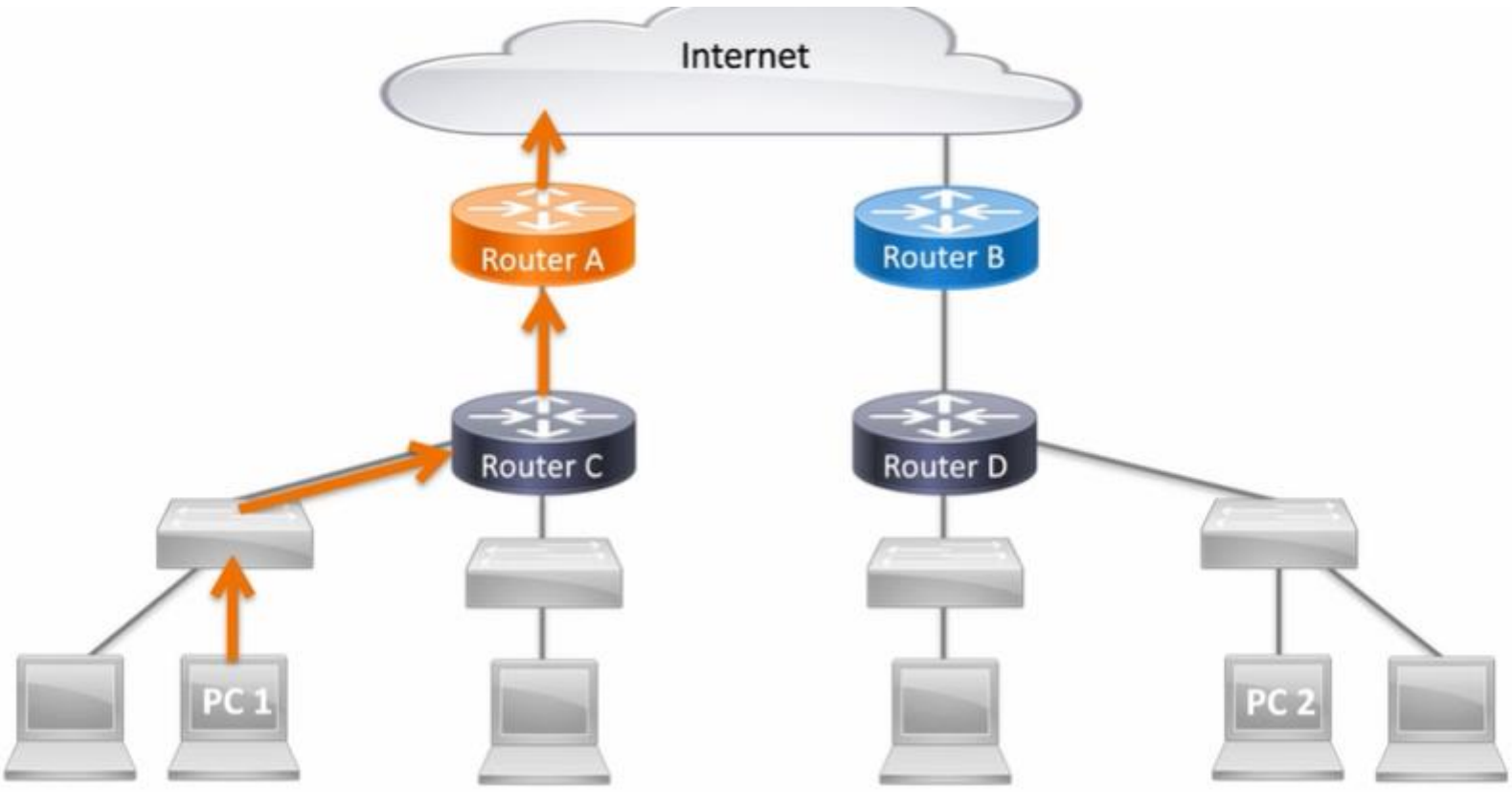
Las redes también admiten una amplia gama de aplicaciones y servicios. Deben operar sobre muchos tipos diferentes de cables y dispositivos, que conforman la infraestructura física. En este contexto, el término arquitectura de red, se refiere a las tecnologías que dan soporte a la infraestructura, a los servicios y a las reglas o protocolos programados que trasladan los datos a través de la red.

A medida que las redes evolucionan, hemos aprendido que hay cuatro características básicas que los arquitectos de redes deben abordar para cumplir con las expectativas del usuario:

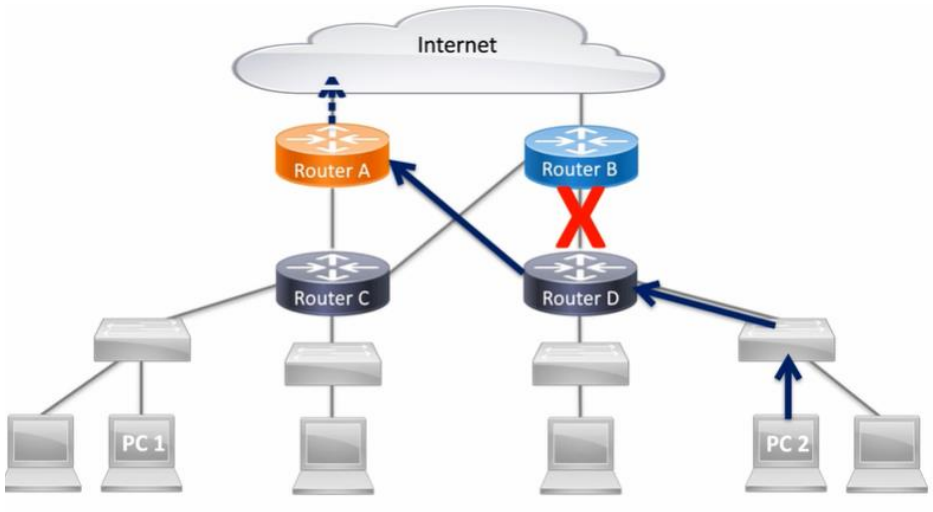
- Tolerancia a fallas
- Escalabilidad
- Calidad de servicio (QoS)
- Seguridad

1.1.2 Vídeo - Tolerancia a Fallas

En este escenario tenemos dos partes en nuestra red, cada una con su propia ruta a nuestro ISP en Internet. Los paquetes que se originan en la PC1 finalmente se reenvían al enrutador A y al ISP, mientras que los paquetes que se originan en la PC2 finalmente se reenvían al enrutador B y luego al mismo ISP. Pero, ¿qué sucede cuando hay un problema con el enrutador A o con un enlace utilizado a lo largo de la ruta al enrutador A? Los paquetes que requieren que el enrutador A los reenvíe a Internet se perderán sin llegar a su destino final. Una red tolerante a fallas es aquella que puede continuar las operaciones sin interrupción cuando uno o más componentes de la red fallan.



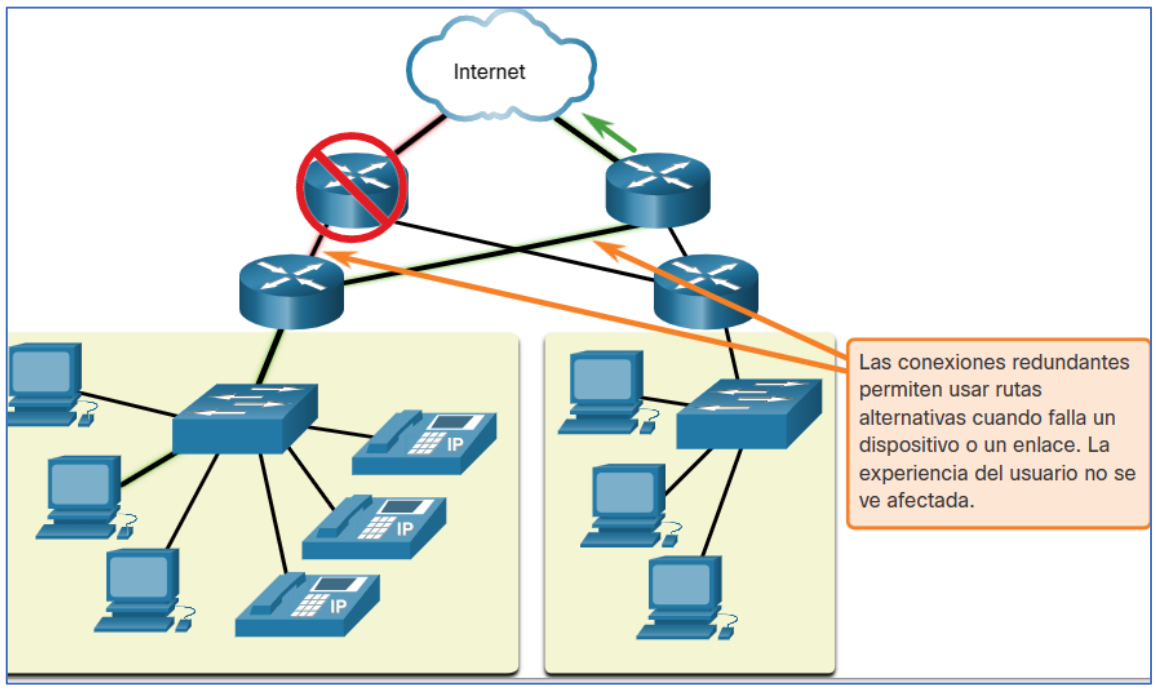
Para ello ahora hemos instalado enlaces adicionales en nuestra red, lo que nos brinda múltiples rutas para llegar a nuestro ISP e Internet. Tener múltiples rutas a un destino se conoce como redundancia, una de las formas de ayudar a que la red sea tolerante a fallas. Si una ruta falla, los paquetes se reenvían automáticamente usando un enlace diferente. Cuanta más redundancia haya en la red, más tolerante a fallas se vuelve la red.



1.1.3 Tolerancia a Fallas

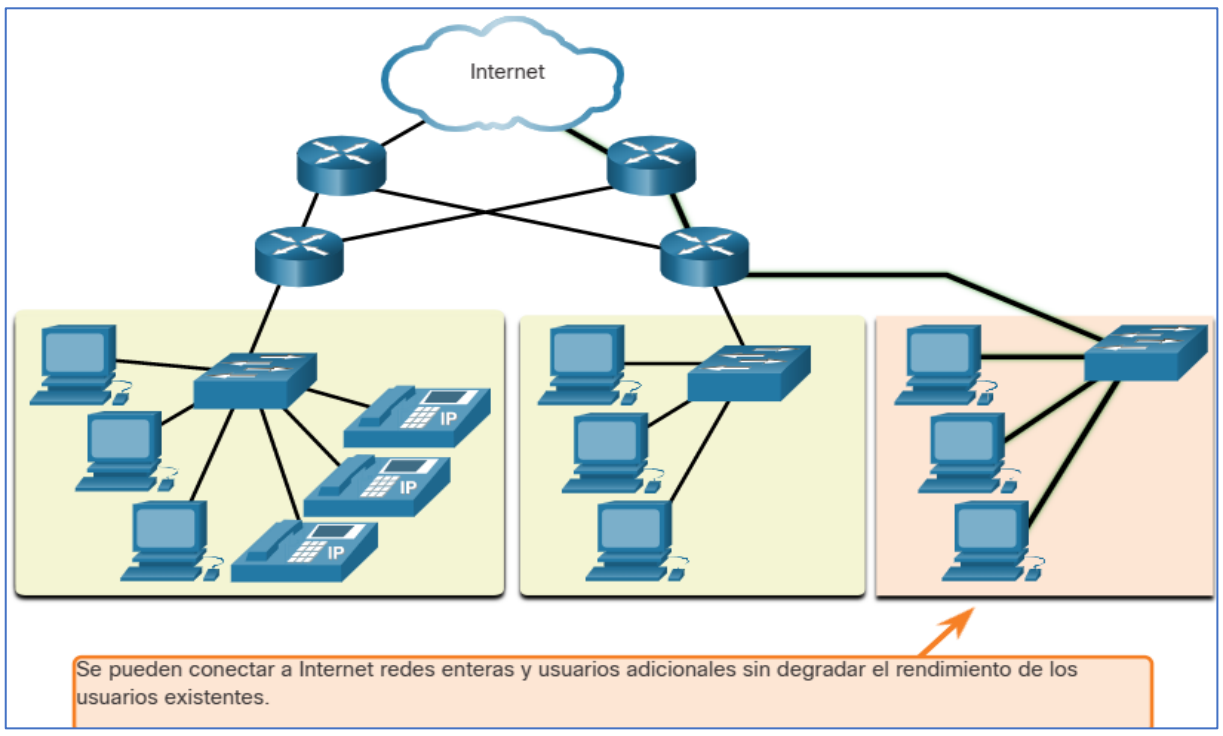
Una red tolerante a fallas es aquella que limita la cantidad de dispositivos afectados durante una falla. Está construido para permitir una recuperación rápida cuando se produce una falla de este tipo. Estas redes dependen de varias rutas entre el origen y el destino del mensaje. Si falla una ruta, los mensajes se pueden enviar inmediatamente por otro enlace. El hecho de que haya varias rutas que conducen a un destino se denomina redundancia.

La implementación de una red de packet-switched (conmutación de paquetes) es una forma en que las redes confiables proporcionan redundancia. La conmutación de paquetes divide el tráfico en paquetes que se enrutan a través de una red compartida. Un solo mensaje, como un correo electrónico o una transmisión de vídeo, se divide en múltiples bloques de mensajes, llamados paquetes. Cada paquete tiene la información de dirección necesaria del origen y el destino del mensaje. Los enrutadores dentro de la red cambian la ruta de los paquetes según la condición de la red en ese momento. Esto significa que todos los paquetes de un mismo mensaje pueden tomar distintas rutas para llegar a su destino. En la figura, el usuario no se da cuenta y no se ve afectado por el cambio dinámico de rutas que hace el enrutador cuando falla un enlace.



1.1.4 Escalabilidad

Una red escalable se expande rápidamente para admitir nuevos usuarios y aplicaciones. Lo hace sin degradar el rendimiento de los servicios a los que están accediendo los usuarios existentes. En la figura, se muestra cómo puede agregarse una red nueva a una red existente con facilidad. En las redes escalables los diseñadores siguen los estándares y protocolos universalmente aceptados. Esto permite a los proveedores de software y hardware centrarse en mejorar los productos y servicios sin tener que diseñar un nuevo conjunto de reglas para operar dentro de la red.

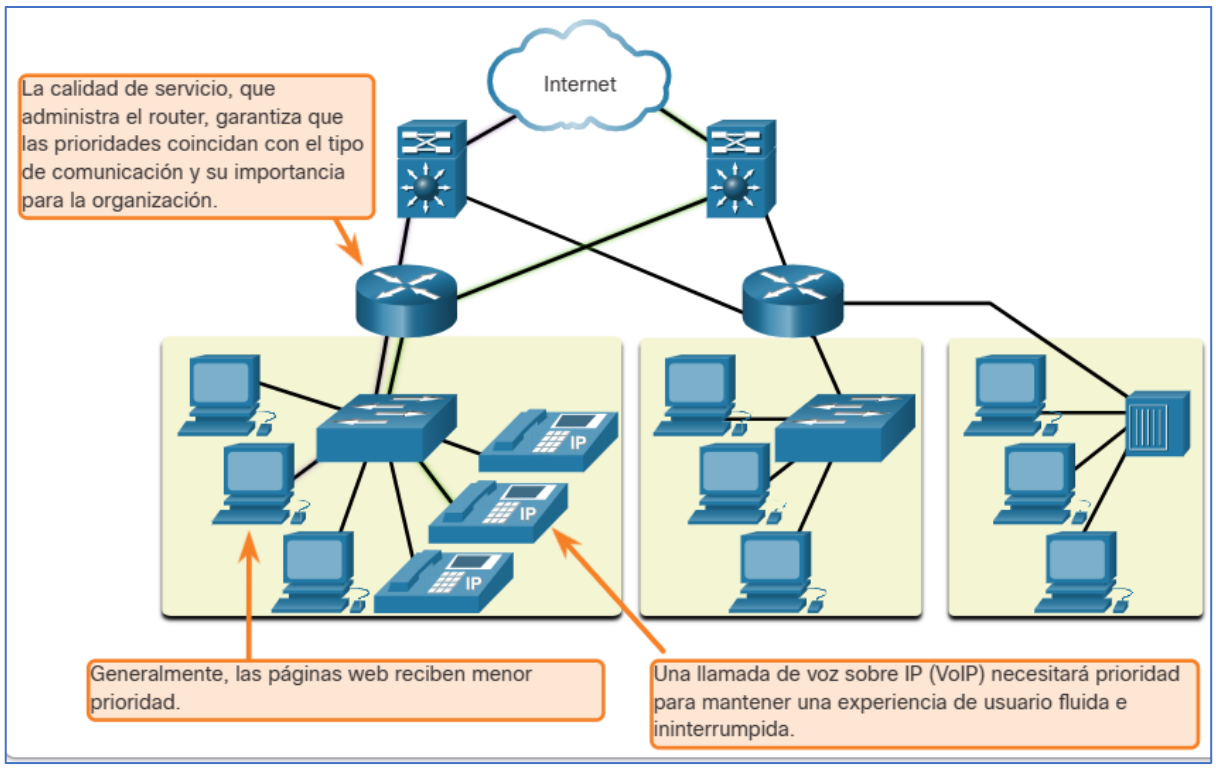


1.1.5 Calidad de Servicio

La calidad de servicio (QoS) es un requisito cada vez más importante para las redes hoy en día. Las nuevas aplicaciones disponibles para los usuarios en internetworks, como las transmisiones de voz y de vídeo en vivo generan expectativas más altas sobre la calidad de los servicios que se proporcionan. ¿Alguna vez intentó mirar un vídeo con interrupciones y pausas constantes? A medida que el contenido de datos, voz y vídeo sigue convergiendo en la misma red, QoS se convierte en un mecanismo principal para administrar la congestión y garantizar el envío confiable de contenido a todos los usuarios.

La congestión se produce cuando la demanda de ancho de banda excede la cantidad disponible. El ancho de banda de la red es la medida de la cantidad de bits que se pueden transmitir en un segundo, es decir, bits por segundo (bps). Cuando se producen intentos de comunicaciones simultáneas a través de la red, la demanda de ancho de banda puede exceder su disponibilidad, lo que provoca congestión en la red.

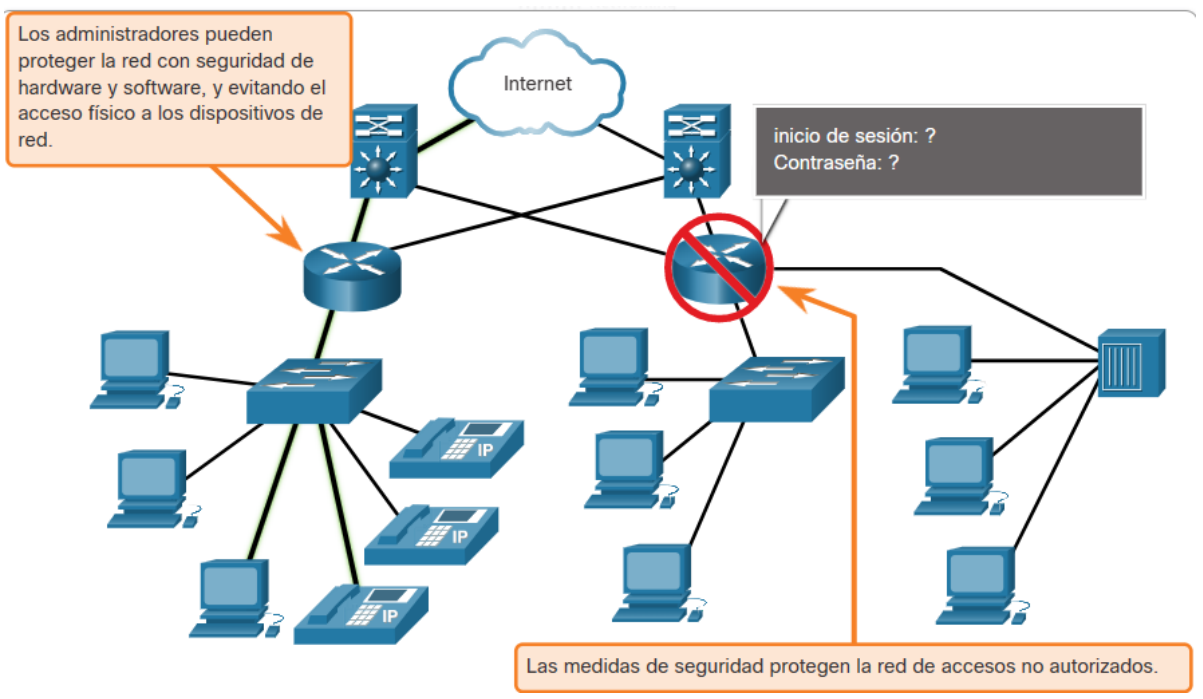
Cuando el volumen de tráfico es mayor de lo que se puede transportar en la red, los dispositivos colocan los paquetes en cola en la memoria hasta que haya recursos disponibles para transmitirlos. En la figura, un usuario solicita una página web y otro está realizando una llamada telefónica. Con una política de QoS, el router puede administrar el flujo de datos y el tráfico de voz, dando prioridad a las comunicaciones de voz si la red se congestiona. El enfoque de QoS es priorizar el tráfico urgente. El tipo de tráfico, no el contenido del tráfico, es lo que importa.



1.1.6 Seguridad de la Red

La infraestructura de red, servicios y datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes. Los administradores de red deben abordar dos tipos de problemas de seguridad de red: seguridad de la infraestructura de red y seguridad de la información.
Asegurar la infraestructura de red incluye asegurar físicamente los dispositivos que proporcionan conectividad de red y evitar el acceso no autorizado al software de administración que reside en ellos, como se muestra en la figura.
Los administradores de red también deben proteger la información contenida en los paquetes que se transmiten a través de la red y la información almacenada en los dispositivos conectados a la red. Para alcanzar los objetivos de seguridad de la red, hay tres requisitos principales:

- **Confidencialidad**- La confidencialidad de los datos se refiere a que solamente los destinatarios deseados y autorizados pueden acceder a los datos y leerlos.
- **Integridad de datos**- Significa tener la seguridad de que la información no ha sido alterada en la transmisión, del origen al destino.
- **Disponibilidad**- Significa tener la seguridad de acceder en forma confiable y oportuna a los servicios de datos para usuarios autorizados.



1.1.7 Verifique su Comprensión - Redes Confiables

Cuando los diseñadores siguen los estándares y protocolos aceptados, ¿cuál de las cuatro características básicas de la arquitectura de red se logra?

Tolerancia a fallas	Escalabilidad ☺←	QoS	Seguridad

La escalabilidad ocurre cuando los diseñadores siguen los estándares y protocolos aceptados.

Confidencialidad, integridad y disponibilidad son requisitos de cuál de las cuatro características básicas de la arquitectura de red

Tolerancia a fallas	Escalabilidad	QoS	Seguridad ☺←

La confidencialidad, la integridad y la disponibilidad son requisitos de seguridad.

¿Con qué tipo de política, un enrutador puede gestionar el flujo de datos y tráfico de voz, dando prioridad a las comunicaciones de voz si la red experimenta congestión?

Tolerancia a fallas	Escalabilidad	QoS ☺←	Seguridad ☺←

QoS significa que un enrutador administrará el flujo de datos y tráfico de voz, dando prioridad a las comunicaciones de voz.

El hecho de que haya varias rutas que conducen a un destino se denomina redundancia. ¿Este es un ejemplo de qué característica de la arquitectura de red?

Tolerancia a fallas ☺←	Escalabilidad	QoS ☺←	Seguridad ☺←

La redundancia es un ejemplo de una arquitectura de red tolerante a fallas.

2. Diseño Jerárquico de Redes

1.2.1 Direcciones Físicas y Lógicas

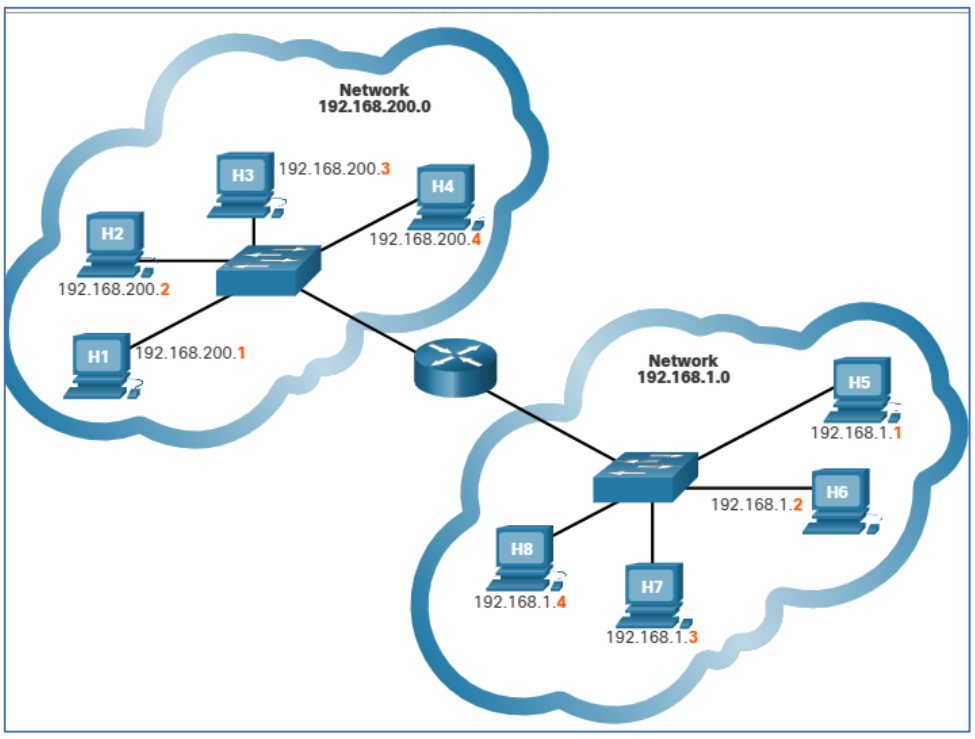
El nombre de una persona generalmente no cambia, pero su dirección puede cambiar.

En un host, su dirección MAC o dirección física es similar al nombre de una persona. Viene asignada a la tarjeta de red (NIC) y será siempre la misma, independientemente del lugar de la red en donde se encuentre el host.

La dirección IP o dirección lógica o dirección de red de un host es similar a la dirección de una persona. Un administrador de red la asigna a cada host en función su ubicación en la red local.

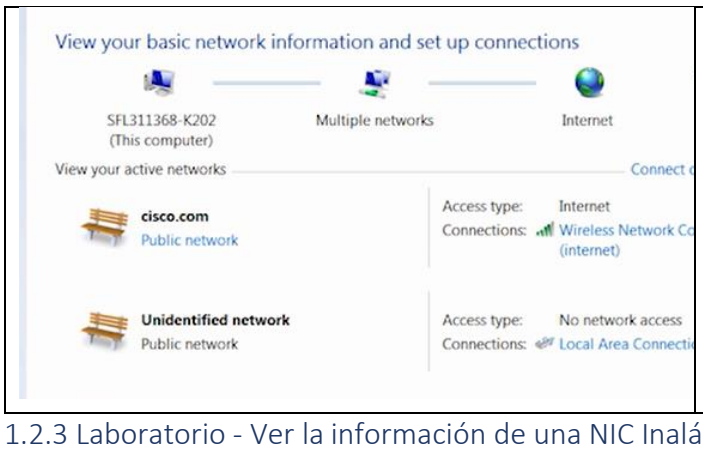
Las direcciones IP contienen dos partes. Una parte identifica la porción de la red. La porción de red de la dirección IP será la misma para todos los hosts conectados a la misma red local. La segunda parte de la dirección IP identifica el host individual en esa red. En la misma red local, la porción de host de la dirección IP es única para cada host, como se muestra en la figura.

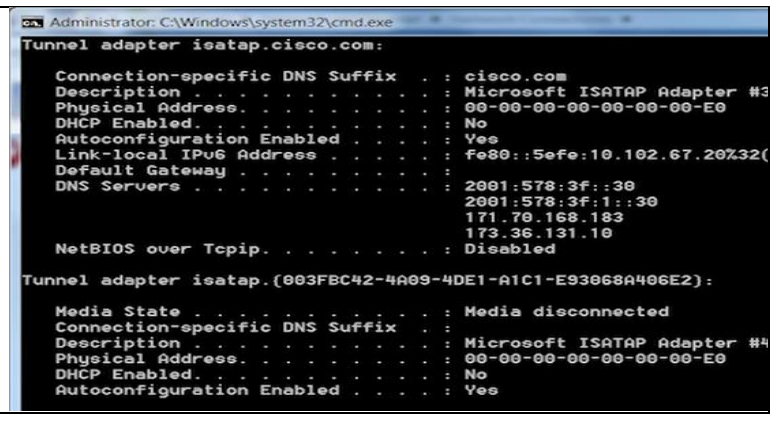
Para que una computadora pueda comunicarse en una red jerárquica, se necesitan tanto la dirección MAC física como la dirección IP lógica, de la misma manera en la que se necesitan el nombre y la dirección de una persona para poder enviarle una carta.



1.2.2 Video - Ver Información de Red en Mi Dispositivo

En este video, veremos cómo obtenemos información de las diversas tarjetas de interfaz de red que se encuentran en nuestras PC. En el caso de esta computadora portátil tengo ambas, una NIC cableada y una NIC inalámbrica. Para ver las propiedades de estos dispositivos voy al ícono de la bandeja del sistema, hago clic derecho y abro el Centro de Redes y Recursos Compartidos. Aparece una lista de conexiones que tengo actualmente activas. Como puede ver, esta es mi computadora y tengo varias redes que se conectan a Internet. Para ver los adaptadores individuales, necesito ir a Cambiar la Configuración del Adaptador. Como puede ver, tengo una Conexión de Area Local (Local Area Connection), que es una conexión por cable. Puedo ver el cable que sale de la parte posterior de mi computadora portátil. También tengo una Conexión de Red Inalámbrica (Wireless Network Connection). Para ver las propiedades de una conexión en particular, todo lo que tiene que hacer es hacer clic con el botón derecho e ir abajo a Propiedades. Hay una serie de propiedades diferentes asociadas a un adaptador de red en una PC con Windows. Por lo general, las que más nos interesan son las configuraciones para el Protocolo de Internet. En este caso, vamos a ver las propiedades de IPv4. Si entramos aquí, podemos ver que nuestro dispositivo está recibiendo su dirección IP automáticamente. Eso significa que está siendo entregado por un servidor DHCP y no estaba configurado estáticamente. Paso a mirar mi adaptador de red con cable, hago exactamente lo mismo, voy a Propiedades elijo IPv4. Puede ver que en este adaptador mi dirección IP se configuró estáticamente, eso significa que un Administrador asignó manualmente la dirección IP a mi PC específicamente. Se puede obtener más información mirando la información Estado de esta conexión en particular. Puedo ver que puedo acceder a Internet. El dispositivo tiene una muy buena señal proveniente del punto de acceso inalámbrico. Si entro en los detalles, incluso puedo obtener más información. Puede ver aquí los diferentes tipos de conexión a los que me dirijo donde obtengo mi DNS. Y mi configuración de DHCP para este adaptador en particular vencerá el miércoles, diciembre el 14 y tendré que renovarlo desde el servidor DHCP. Puedo obtener información sobre la dirección MAC, sobre el tipo de conexión y las redes inalámbricas en las que estoy conectado. En la conexión de área local, la información Estado que se ve es ligeramente diferente. Te dice ahora mismo que en el caso de mi red cableada no voy a poder salir más allá del primer nivel superior de mi red y que mi conexión en sí está habilitada y es de 100 megabytes. Nuevamente, tenemos los detalles donde puedo obtener mi MAC y mi dirección IPv4. Y si tuviera una dirección IPv6 configurada, también se mostraría. Ahora, la mayor parte de esta información que ve en Estado del controlador NIC también se puede ver yendo al Símbolo del Sistema de Windows y corriendo el comando ***ipconfig***. Este comando tiene varias opciones, la más utilizada es ***/all***, que brinda mucha información sobre cómo está configurado su dispositivo. Como puede ver aquí, aquí están mis adaptadores que tengo para la conexion inalámbrica y para la conexión por cable. Es una práctica común encontrar la dirección MAC, la dirección IP y el estado actual del adaptador de PC. Así que esta es una habilidad que obtendrán con mucha práctica.





1.2.3 Laboratorio - Ver la información de una NIC Inalámbrica y Cableada

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Identificar y trabajar con NICs de PC
- Identificar y utilizar los íconos de red de la bandeja del sistema

Laboratorio: Ver la información de una NIC inalámbrica y cableada

Objetivos

Parte 1: Identificar y trabajar con NIC de PC

Parte 2: Identificar y utilizar los iconos de red de la bandeja del sistema

Información básica/situación

Este laboratorio requiere determinar la disponibilidad y el estado de las tarjetas de interfaz de red (NIC) en la PC. Windows proporciona diversas maneras de ver y de trabajar con las NIC.

En este laboratorio, accederá a la información de NIC de la PC y cambiará el estado de estas tarjetas.

Recursos necesarios

- 1 PC (Windows 10 con dos NIC, cableada e inalámbrica, y una conexión inalámbrica)
- Un enrutador inalámbrico

Instrucciones

Parte 1: Identificar y trabajar con NIC de PC

En la parte 1, identificará los tipos de NIC que posee la PC. Explorará las diferentes formas de extraer información acerca de estas NIC y cómo activarlas y desactivarlas.

Nota: Este laboratorio se realizó utilizando una PC que se ejecuta en el sistema operativo Windows 10. Es posible realizar el laboratorio con otra versión del sistema operativo Windows. Sin embargo, las opciones de los menús y las pantallas pueden variar.

Paso 1: Usar conexiones de red.

Verificará qué conexiones de red están disponibles.

a. Haga clic con el botón secundario del mouse en **Start** (Inicio) y seleccione **Network Connections** (Conexiones de red).

b. La ventana Conexiones de red muestra la lista de NIC disponibles en esta PC. En esta ventana, busque los adaptadores de conexión de área local y conexión de red inalámbrica.

Nota: Si aparece la página de estado de la red, haga clic en **Change adapter options** (Cambiar opciones de adaptador) para desplazarse hasta la ventana Conexiones de red.

Nota: Es posible que en esta ventana también figuren otros tipos de adaptadores de red, como el adaptador de conexión de red Bluetooth y de red privada virtual (VPN).

Paso 2: Trabajar con la NIC inalámbrica.

Verifique la configuración de la conexión de red inalámbrica.

a. Haga clic con el botón derecho en una **Wireless Network Connection** (Conexión de red inalámbrica). La primera opción muestra si la NIC inalámbrica está habilitada o deshabilitada. Si la NIC inalámbrica está deshabilitada, la opción **Activar**le permitirá habilitarla.

b. Verifique que la red inalámbrica esté conectada. De lo contrario, haga clic en **Connect/Disconnect** (Conectar/Desconectar) para conectarse a la red deseada. Haga clic en **Estado** para abrir la ventana Estado de la conexión de red inalámbrica.

¿Cuál es el Identificador de conjunto de servicios (SSID) para el enrutador inalámbrico de la conexión?
Las respuestas pueden variar. El SSID es el nombre principal asociado a la red de área local inalámbrica (WLAN). Estas redes WLAN pueden ser redes inalámbricas domésticas o zonas públicas. El SSID se utiliza para identificar el nombre de la red inalámbrica.

¿Cuál es la velocidad de la conexión inalámbrica?
Las respuestas pueden variar. Esta velocidad de conexión inalámbrica indica la velocidad entre el enrutador inalámbrico y la NIC en su PC, no la velocidad proporcionada por el proveedor de servicios de Internet (ISP).

c. Haga clic en Detalles para visualizar la ventana Detalles de la conexión de red.

¿Cuál es la dirección MAC de la NIC inalámbrica?
Las respuestas pueden variar. La dirección MAC es el identificador único asignado a la NIC inalámbrica.

d. Abra la línea de comandos (Command Prompt) e introduzca el comando ***ipconfig /all.***

C:\Usuarios\Roberto> ***ipconfig /all***

Observe que la información que se muestra es similar a la información de la ventana de Detalles de la conexión de red. Cuando haya revisado los detalles, haga clic en Cerrar para volver a la ventana Estado de la conexión de red inalámbrica.

e) Vuelva a la ventana Estado de la conexión de red inalámbrica. Haga clic en **Propiedades inalámbricas** para abrir la ventana **Propiedades de red inalámbrica** de la red **Home-Net.**

f) Siempre que la seguridad inalámbrica esté disponible, debe usarla. Para verificar (o configurar) las opciones de seguridad inalámbrica, haga clic en la ficha **Seguridad**. La ventana muestra el tipo de seguridad y el método de encriptación habilitados. En esta ventana, también puede introducir (o cambiar) la clave de seguridad. Cierre todas las ventanas.

Paso 3: Trabaje con la NIC conectada por cable.

Ahora verificaremos la configuración de la conexión de red cableada.

a. Abra la ventana **Conexiones de red** haciendo clic con el botón secundario del mouse en **Inicio** de Windows > **Conexiones de red**.

Nota: Si aparece la página de estado de la red, haga clic en **Cambiar opciones de adaptador** para desplazarse hasta la ventana Conexiones de red.

b. Seleccione y haga clic sobre la opción **Conexión de área local** para ver la lista desplegable. Si la NIC está deshabilitada, habilítela.

c. Haga clic en la opción **Estado** para abrir la ventana Estado de la conexión de área local. Esta ventana muestra información acerca de la conexión por cable a la LAN.

d. Haga clic en **Detalles...** para ver la información de la dirección para la conexión LAN.

e. Abra la línea de comandos (Command Prompt) e introduzca el comando **ipconfig /all**. Busque la información de la conexión de área local y compárela con la información que se muestra en la ventana Detalles de la conexión de red.

f. Cierre todas las ventanas del escritorio.

Parte 2: Identifique y utilice los íconos de red de la bandeja del sistema

En la parte 2, usará los íconos de red de la bandeja del sistema para mostrar las redes disponibles en la red.

a. La esquina inferior derecha de la pantalla de Windows 10 contiene la bandeja del sistema. Mueva el mouse para mostrar la bandeja del sistema.

b. Si pasa el cursor sobre el icono de red en la bandeja del sistema, se muestran las redes conectadas actualmente.

c. Haga clic en el ícono de la red inalámbrica y verá los SSID de red cableada e inalámbrica que se encuentran dentro del alcance de la NIC inalámbrica.

d. Al hacer clic con el botón secundario del mouse en el ícono de la red inalámbrica, aparece una opción de solución de problemas y se abre la ventana del Centro de redes y recursos compartidos.

e. Haga clic en la opción **Abrir Centro de redes y recursos compartidos** (Open Network and Sharing Center).

f. El Centro de redes y recursos compartidos es una ventana central que muestra información sobre la red o las redes activas, el tipo de red, el tipo de acceso.

Reflexión:

¿Por qué activaría más de una NIC en una PC?

Las respuestas pueden variar. Se pueden utilizar varias NIC si se necesita más de una ruta para la PC. Un ejemplo de esto sería si la PC se utiliza como servidor proxy.

1.2.4 Analogía Jerárquica

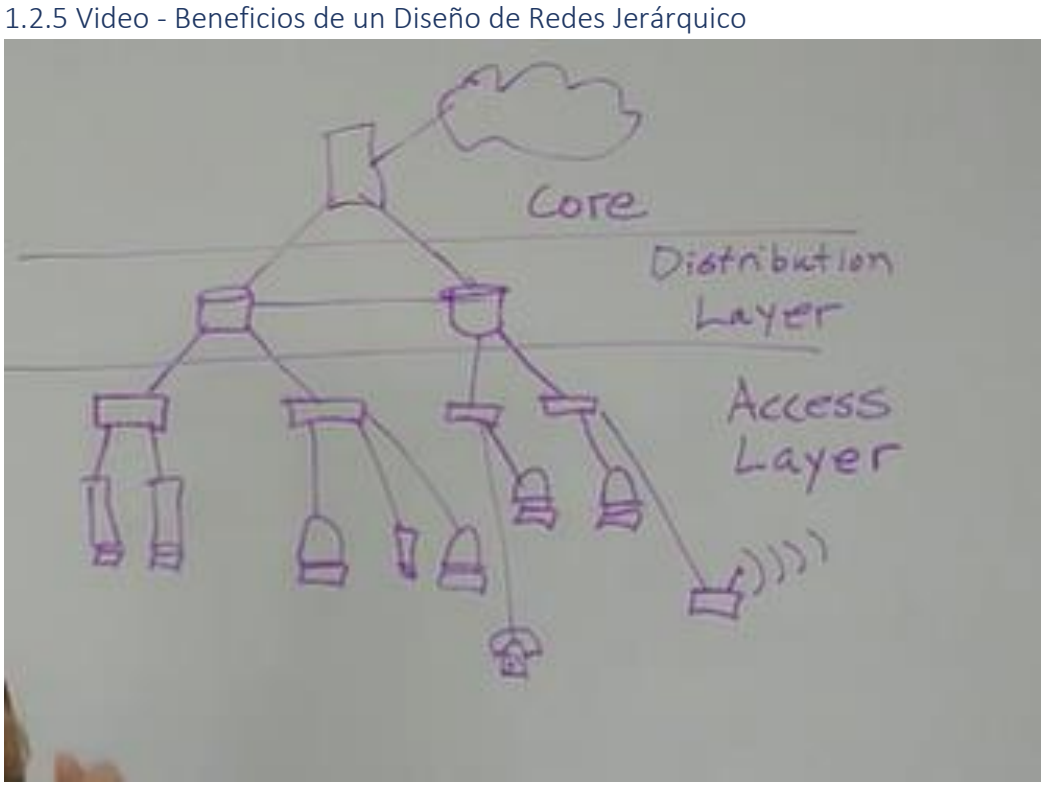
Imagine lo difícil que sería la comunicación si la única manera de enviar un mensaje a alguien fuera utilizar el nombre de la persona. Si no hubiera direcciones, ciudades, pueblos o países, la entrega del mensaje a una persona específica en algún lugar del mundo sería prácticamente imposible.

En una red Ethernet, la dirección MAC del host es similar al nombre de una persona. Una dirección MAC indica la identidad individual de un host específico, pero no indica en qué lugar de la red se encuentra el host. Si todos los hosts en Internet (millones y millones de ellos) fueran identificados solo por su dirección MAC única, imagine lo difícil que sería localizar uno en particular.

Además, la tecnología Ethernet genera una gran cantidad de tráfico de difusión para que los hosts se comuniquen. Las difusiones se envían a todos los hosts de una única red. Las difusiones consumen ancho de banda y afectan el rendimiento de la red. ¿Qué ocurriría si los millones de hosts conectados a Internet estuvieran todos en una red Ethernet y utilizaran difusiones?

Por estos dos motivos, no es eficaz utilizar grandes redes Ethernet con muchos hosts. Es mejor dividir las redes más grandes en partes más pequeñas y fáciles de administrar. Una manera de dividir redes grandes es utilizar un modelo de diseño jerárquico.

1.2.5 Video - Beneficios de un Diseño de Redes Jerárquico



En este video, hablaremos sobre los beneficios del diseño jerárquico al planificar una red. Por lo general, las redes crecen de forma orgánica, comenzamos con un dispositivo pequeño y algunas estaciones de trabajo. Piense en su red doméstica, un par de computadoras y otros dispositivos, tal vez una impresora, una consola de juegos. Imagine un negocio hogareño cuya red necesita crecer con algunos dispositivos adicionales como escáneres e impresoras. Así que podría tener un escáner aquí y tal vez otra impresora. Y luego, de repente, me di cuenta de que mi pequeño dispositivo de red doméstico ya no tiene suficientes puertos para admitir todos mis diversos dispositivos. A medida que crece mi pequeña empresa y remodelamos el garaje para instalarlo, ahora tengo que tener otro dispositivo. Y generalmente conectamos ese dispositivo al otro dispositivo y luego la red comienza a crecer orgánicamente. Esto es cierto para su red doméstica, pero también es cierto para las redes empresariales. Muchas veces, las empresas de todos los tamaños no piensan en cómo están creando su red, simplemente permiten que crezca a medida que necesitan más dispositivos en la red. Pero muy pronto terminamos con una red que tiene dispositivos de misión crítica, por ejemplo, un servidor al que sus clientes necesitaban acceder, junto con cosas secundarias para este tipo de tráfico que podrían interferir con él, como la consola de juegos o alguien descargando una película. Una red que simplemente crece orgánicamente muchas veces no es eficiente. Con el tiempo, un tipo de arquitectura de red se ha convertido prácticamente en el estándar y se llama **diseño de red jerárquico**. En un diseño jerárquico, pensamos cómo organizar nuestra red para que tengamos cosas importantes como servidores críticos. Las redes jerárquicas pueden escalar porque están diseñadas lógicamente, de manera que el tráfico que debe ir de ciertas personas a ciertos servidores, no necesita viajar a las áreas de la red donde no sea necesario. Ahora, una pequeña discusión sobre la transmisión. Los paquetes de transmisión van a todos los dispositivos (pueden ser cientos) que están en la misma red local, es decir, la misma área de la red que solo está conectada por interruptores. Entonces, todo el tráfico generado por estos dispositivos permanecerá en esta área, la red. Entonces, la escala de la red jerárquica es bastante buena. Ahora, cuando la red jerárquica necesita conectarse a otras redes, tendremos otros dispositivos que brindan la conectividad para salir a Internet. En un diseño de red jerárquico, se dan nombres a estas diversas capas. Dispositivos que realmente conectan a los usuarios y otros dispositivos de usuarios finales residen en la **Capa de Acceso**. La función principal de la capa de acceso de la red es proporcionar un punto de entrada para que los dispositivos ingresen a la red, por ejemplo, computadoras de los usuarios finales, iPhones, puntos de acceso, servidores y servicios que se proporcionan en esta capa. La siguiente capa es la **Capa de Distribución** cuya función principal es interconectar las redes de la capa de acceso, tal que el tráfico que debe permanecer local permanece local y el tráfico que debe atravesar redes remotas en realidad tiene una ruta para usar para ir de una red a otra. Ahora, por encima de todo eso está la **Capa Core** o **Capa Central** o **Núcleo** responsable para el procesamiento de alta velocidad. Entonces, en este caso, tenemos a todos nuestros usuarios que necesitan acceder a Internet, nuestra capa central se encargará de agregar todo el tráfico que proviene de estos dispositivos y asegurarse de que se transmita de manera eficiente a través de los enlaces **WAN** a Internet. Básicamente, esta es una de las razones principales por las que necesitamos pensar en la planificación de nuestras redes antes de construirlas. En realidad, no es de importancia crítica cuando está construyendo una red doméstica, pero en una red que necesita estar activa y operativa la mayor parte del tiempo debe tener un diseño tal que una falla de un componente no impactará al resto de la red.

1.2.6 Acceso, Distribución y Núcleo

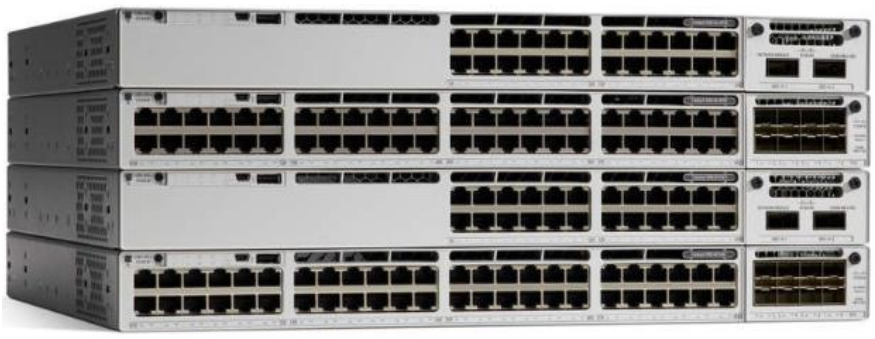
El tráfico IP se administra basándose en las características y los dispositivos asociados con cada una de las tres capas del modelo de diseño de redes jerárquico: Acceso, Distribución y Núcleo.

Capa de Acceso

La capa de acceso proporciona un punto de conexión a red para los dispositivos de usuarios finales y permite que varios hosts se conecten a otros hosts a través de un conmutador, como el Cisco 2960-XR que se muestra en la figura, o un punto de acceso inalámbrico. Normalmente, la porción de red de la dirección IP será la misma para todos los dispositivos de una misma capa de acceso.

Si un mensaje está destinado a un host local, según indique la porción de red de la dirección IP, el mensaje permanecerá en el nivel local. Si está destinado a una red diferente, pasa a la capa de distribución. Los enrutadores y conmutadores de Capa 3 proporcionan conexión a los dispositivos de la capa de distribución.

Capa de Distribución



La capa de distribución proporciona puntos de conexión para redes diferentes y controla el flujo de información entre ellas. Contiene enrutadores y conmutadores potentes como la serie Cisco C9300. Los dispositivos de la capa de distribución controlan el tipo y la cantidad de tráfico que circula desde la capa de acceso hasta la capa principal o Core.

Cisco de la Serie C9300

Capa de Núcleo

La capa de núcleo es una capa troncal de alta velocidad con conexiones redundantes (de respaldo). Es la encargada de transportar grandes cantidades de datos entre múltiples redes finales. Los dispositivos de capa de núcleo suelen incluir enrutadores y conmutadores potentes de alta velocidad, como el Cisco Catalyst 9600 que se muestra en la figura. El objetivo principal de la capa de núcleo es transportar datos con rapidez.

Cisco Catalyst 9600

1.2.7 Verifique su Comprensión - Diseño de Redes Jerárquico

Una dirección IP se considera qué tipo de dirección

Física	Lógica ☺←

Una dirección IP es una dirección lógica.

Una dirección MAC de Ethernet se considera qué tipo de dirección

Física ☺←	Lógica

Una dirección MAC de Ethernet es una dirección física.

¿Cuál dirección no cambia cuando un dispositivo se conecta a una nueva red?

Física ☺←	Lógica

La dirección física no cambia cuando el dispositivo se conecta a una nueva red.

¿Cuál capa del diseño proporciona conectividad a los dispositivos en una LAN Ethernet?

Núcleo	Distribución	Acceso ☺←	Física

La capa de acceso proporciona conectividad a dispositivos en una LAN Ethernet

¿Qué parte de una dirección IP identifica de manera exclusiva ese dispositivo en esa red?

Física	Lógica	Red	Host ☺←

La porción de host de una dirección IP identifica de manera única ese dispositivo en esa red.

3. Resumen de diseño de redes

1.3.1 ¿Qué Aprendí en este Módulo?

Redes Confiables

A medida que las redes evolucionan, hemos aprendido que hay cuatro características básicas que los arquitectos de redes deben abordar para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, QoS y seguridad.

Una red tolerante a fallas limita la cantidad de dispositivos afectados durante una falla. Permite una recuperación rápida cuando ocurre una falla de este tipo. Estas redes dependen de varias rutas entre el origen y el destino del mensaje. Si falla una ruta, los mensajes se pueden enviar inmediatamente por otro enlace.

Una red escalable se expande rápidamente para admitir nuevos usuarios y aplicaciones. Lo hace sin degradar el rendimiento de los servicios a los que están accediendo los usuarios existentes. Las redes pueden ser escalables si los diseñadores siguen los estándares y protocolos aceptados.

QoS es un requisito cada vez mayor de las redes hoy en día. A medida que el contenido de datos, voz y vídeo sigue convergiendo en la misma red, QoS se convierte en un mecanismo principal para administrar la congestión y garantizar el envío confiable de contenido a todos los usuarios. El ancho de banda de la red se mide en bps. Cuando se producen intentos de comunicaciones simultáneas a través de la red, la demanda de ancho de banda puede exceder su disponibilidad, lo que provoca congestión en la red. El enfoque de QoS es priorizar el tráfico urgente. El tipo de tráfico, no el contenido del tráfico, es lo que importa.

Los administradores de red deben abordar dos tipos de problemas de seguridad de red: seguridad de la infraestructura de red y seguridad de la información. Los administradores de red también deben proteger la información contenida en los paquetes que se transmiten a través de la red y la información almacenada en los dispositivos conectados a la red. Hay tres requisitos principales para lograr los objetivos de la seguridad de la red: Confidencialidad, Integridad y Disponibilidad.

Diseño de Redes Jerárquico

Las direcciones IP contienen dos partes. Una parte identifica la porción de la red, que será la misma para todos los hosts conectados a la misma red local. La segunda parte de la dirección IP identifica el host individual en esa red. Se requieren tanto la dirección MAC física como la dirección IP lógica para que una computadora se comunique en una red jerárquica.

El Centro de Redes y Recursos Compartidos en una PC muestra la información básica de la red y las conexiones de configuración, incluidas las redes activas y si está conectado por cable o de forma inalámbrica a Internet y dentro de su LAN. Puede ver las propiedades de las conexiones aquí.

En una red Ethernet, la dirección MAC del host es similar al nombre de una persona. Una dirección MAC indica la identidad individual de un host específico, pero no indica en qué lugar de la red se encuentra el host. Si todos los hosts en Internet (millones y millones de ellos) fueran identificados solo por su dirección MAC única, imagine lo difícil que sería localizar uno en particular. Es mejor dividir las redes más grandes en partes más pequeñas y fáciles de administrar. Una manera de dividir redes grandes es utilizar un modelo de diseño jerárquico.

Las redes jerárquicas escalan bastante bien. La **capa de acceso** proporciona un punto de conexión a la red para los dispositivos de usuarios finales y permite que varios hosts se conecten a otros hosts a través de un dispositivo de red, por lo general un conmutador o un punto de acceso inalámbrico. Normalmente, la porción de red de la dirección IP será la misma para todos los dispositivos de la misma capa de acceso. La **capa de distribución** proporciona un punto de conexión para redes independientes entre sí y controla el flujo de información entre las redes. Los dispositivos de la capa de distribución controlan el tipo y la cantidad de tráfico que circula desde la capa de acceso hasta la capa principal. La **capa de núcleo** es una capa troncal de alta velocidad con conexiones redundantes. Es la encargada de transportar grandes cantidades de datos entre múltiples redes finales. El objetivo principal de la capa principal es transportar datos con rapidez.

1.3.2 Webster - Preguntas de Reflexión

Marcy y Vincent tienen la suerte de que Bob consulte con ellos sobre la red en su tienda. Muchas pequeñas empresas tienen redes que crecen con el tiempo, pero no están diseñadas para escalar de manera confiable o segura. Marcy y Vincent comprenden que, si se toman el tiempo y gastan dinero ahora, se ahorrarán muchos problemas a medida que su red continúa creciendo. Sabiendo lo que sabe ahora sobre redes confiables y escalables, ¿hay algo que le gustaría hacer para actualizar su propia red en el hogar, la escuela o el trabajo?

1.3.3 Prueba de Diseño de Redes

¿Cuáles dos dispositivos se encuentran comúnmente en la capa de acceso del modelo jerárquico de diseño de LAN empresarial? (Elija dos opciones).

Punto de acceso ☺←	Cortafuegos	Conmutador de capa 2 ☺←	Dispositivo de capa 3	Conmutador modular

¿Qué característica de una red le permite expandirse rápidamente para admitir a nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio que se les proporciona a los usuarios actuales?

Confiabilidad	Escalabilidad ☺←	Calidad de servicio	Accesibilidad

Un estudiante está transmitiendo una película a su computadora, pero la película se detiene. ¿Qué servicio daría mayor prioridad al tráfico de transmisión y evitaría que la película se detenga?

HTTPS	Seguridad	Tolerancia a fallas	QoS ☺←

¿Verdadero o falso? El impacto de la falla de un dispositivo de red importante puede verse limitado por una función llamada tolerancia a fallas.

Verdadero ☺←	Falso

¿Qué tipo de dirección nunca cambia en un dispositivo y es similar a una dirección particular?

Dirección MAC ☺←	Dirección IP	Dirección de Red	Dirección lógica

¿Cuáles son las tres capas de un modelo de diseño de redes jerárquico? (Elija tres opciones).

Acceso ☺←	Enlace de datos	Núcleo ☺←
Acceso a la red	Empresarial	Distribución ☺←

¿Qué función de red utiliza la redundancia como medio para limitar la cantidad de usuarios afectados en caso de falla?

Tolerancia a fallas ☺←	Escalabilidad	QoS	Seguridad

¿Qué característica de una red permitiría que el tráfico de video tenga prioridad sobre el tráfico de una aplicación de correo electrónico?

Tolerancia a fallas	Escalabilidad	QoS ☺←	Seguridad

¿Cuál modelo de diseño de redes mejora la eficiencia al dividir la red en partes más pequeñas?

Jerárquico ☺←	Redundante	Tolerancia a fallas	Confiable

Haga coincidir la función con la descripción

escalabilidad	✓ proporciona confiabilidad
calidad de servicio	✓ permite que la red crezca
tolerancia a fallas	✓ priorizar el tráfico

Una la definición con el objetivo de seguridad.

garantizando la confidencialidad	✓ solo los destinatarios previstos pueden acceder y leer los datos
manteniendo la integridad	✓ la seguridad de que la información no ha sido alterada durante la transmisión
asegurando la disponibilidad	✓ la garantía de un acceso oportuno y fiable a los datos

¿Cuál es la responsabilidad de la capa de distribución en un diseño de redes jerárquico?

Controla el flujo de tráfico entre las otras capas ☺←	Proporciona acceso a la red a los usuarios finales	Proporciona una red troncal de alta velocidad para los flujos de trafico	Controla que dispositivos pueden comunicarse en la red

Módulo 2: La Nube y Virtualización

0. Introducción

2.0.1 Webster - ¿Por Qué Debería Tomar este Módulo?

Al planificar la red futura, Bob cree que Marcy y Vincent deben aprovechar los servicios en la nube y la virtualización. Bob explicó que pueden arrendar servicios de un proveedor de la nube. Marcy y Vincent querían saber por qué deberían considerar esto. Bob explica que esto consumirá menos energía, requerirá menos equipos y menos espacio. También puede ayudar con la recuperación tras un desastre. Compara esto con las imágenes de Marcy y Vincent en sus teléfonos móviles respaldadas en una nube. Incluso si el teléfono móvil se daña, las fotos aún pueden recuperarse. ¿Puede pensar en cómo utiliza la nube? ¿Cuánto sabe sobre la nube y la virtualización? Permítame ayudarlo a aprender más. ¡Aproveche este módulo!

2.0.2 - ¿Qué Aprenderé en este Módulo?

Título del módulo: La Nube y Virtualización

Objetivo del Módulo: Explicar las características de la virtualización y los servicios en la nube.

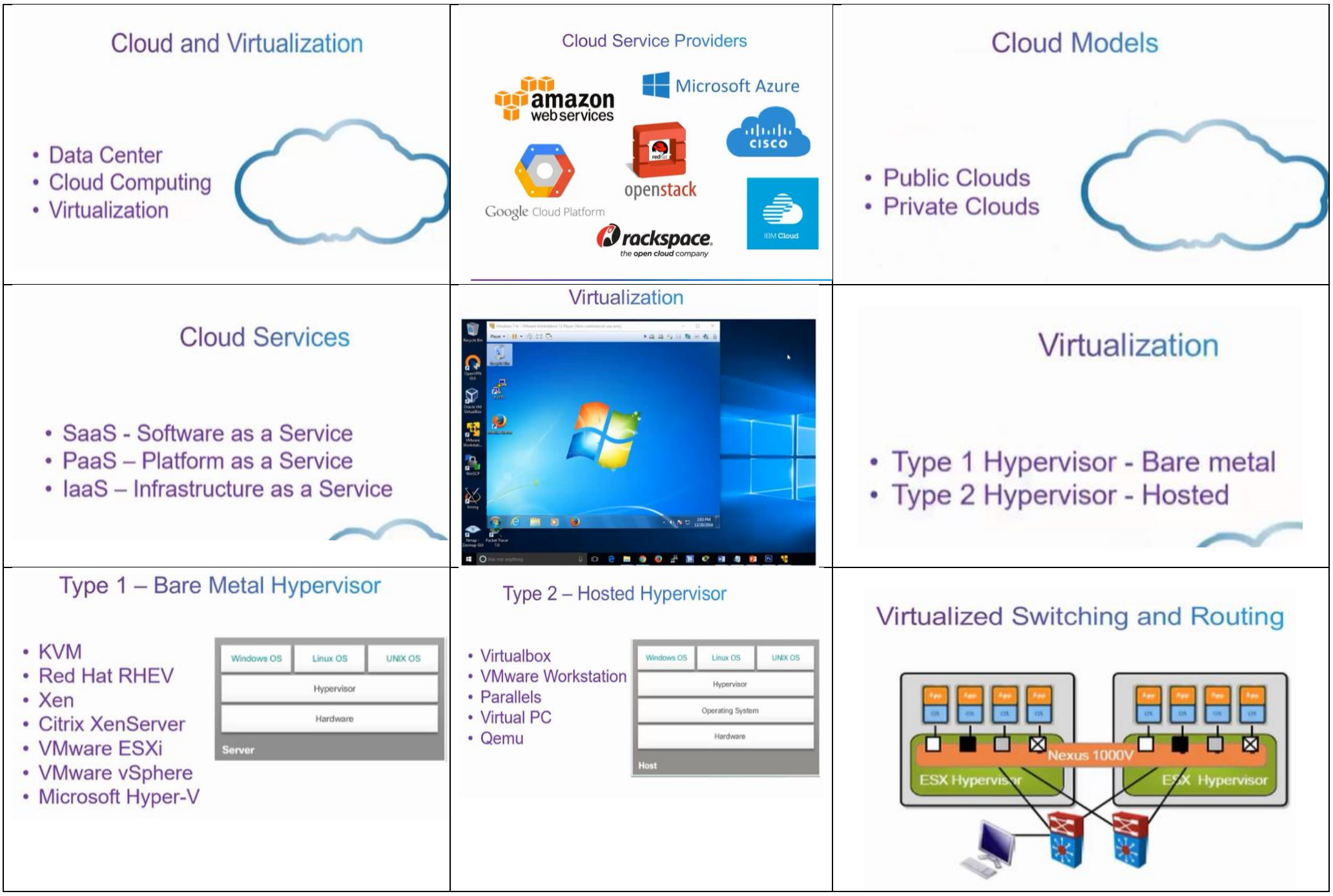
Título del Tema	Objetivo del Tema
La Nube y Servicios en la Nube	Explicar las características de las nubes y los servicios en la nube.
Virtualización	Explicar el propósito y las características de la virtualización

1. La nube y servicios en la nube

2.1.1 Vídeo - La Nube y Virtualización

En general, cuando hablamos de la nube, nos referimos a tres cosas: Centros de Datos (Data Centers), Computación en la Nube (Cloud Computing) o Servicios en la Nube (Cloud Services) y Virtualización o Computación Virtual (Virtual Computing). Aunque los centros de datos pueden ser más pequeños, por lo general son instalaciones grandes que proporcionan cantidades masivas de energía, enfriamiento y ancho de banda. Solo organizaciones muy grandes como Facebook o Google pueden permitirse construir sus propios centros de datos privados para brindar servicios a sus usuarios. Otras organizaciones más pequeñas arriendan espacio de un Centro de Datos. Los proveedores de servicios en la nube como Cisco, Amazon Web Services o Microsoft Azure ofrecen sus servicios fuera de los Centros de Datos. Hay dos tipos básicos de nubes, públicas y privadas. Las nubes públicas ofrecen servicios y aplicaciones para la población en general, mientras que las nubes privadas están destinadas a organizaciones o entidades específicas, como gobiernos, y solo esas organizaciones privadas acceden a ellas. Hay diferentes categorías de servicios en la nube, SaaS o Software como Servicio que se refiere al software bajo demanda o un modelo de suscripción donde la licencia y la entrega del software se realiza a través de la nube. Encontrará esto en Office 365 o Adobe Creative Cloud o incluso en software de juegos de computadora, en ellos el acceso al software ocurre generalmente a través de un navegador web. Generalmente el software no tiene propietarios sino se alquila. PaaS o Plataforma como Servicio, es donde el proveedor de servicios en la nube proporciona la plataforma, como la plataforma Java o .NET para que un desarrollador desarrolle una aplicación, por ejemplo un aplicativo para celulares (app). Esto generalmente implica proporcionar bases de datos y herramientas al desarrollador para que pueda desarrollar rápidamente una aplicación para celulares. IaaS o Infraestructura como Servicio se refiere a Computación Virtual que se puede proporcionar a través de Internet bajo demanda. Esto incluye elementos de computación virtual, como servidores virtuales, así como almacenamiento virtualizado y capacidades de red virtualizadas que se pueden aprovisionar, asignar y suministrar a pedido según sea necesario. La virtualización es la capacidad de abstraer o separar el sistema operativo del hardware físico. Para crear una computadora virtual, el hardware físico exclusivo o dedicado debe compartirse con la computadora virtual. En esta diapositiva, vemos una computadora virtual con Windows 7 que está compartiendo recursos físicos dedicados de la computadora host, esto se hace a través de un hipervisor. Se utilizan dos tipos de hipervisores en la virtualización, el Tipo 1 conocido como hipervisor Bare Metal instalado directamente en el hardware, y el Tipo 2 conocido como hipervisor Hosted o Alojado. El Tipo 1 Bare Metal es un servidor de

virtualización. El hipervisor es un sistema operativo instalado directamente en el hardware, luego se crean las computadoras virtuales. Existen diferentes tipos de hipervisores Tipo 1 como KVM, Red Hat Enterprise Virtualization, Xen, Citrix XenServer, VMware ESXi, VMware vSphere y Microsoft Hyper-V. El hipervisor Tipo 2 se conoce como hipervisor alojado. En esta situación, el hipervisor es una aplicación o programa que se instala sobre el sistema operativo del host. En otras palabras, se instala el hipervisor como VirtualBox o VMware Workstation, Parallels, Virtual PC en el nivel alto de la computadora host. Instala VirtualBox digamos, sobre el sistema operativo Windows, y luego puede crear computadoras virtuales. Además de la computación virtual, también podemos virtualizar la conmutación y el enrutamiento. En esta diapositiva podemos ver dos hipervisores VMware y ESxi, todas las computadoras virtuales están conectadas en red con un conmutador virtual Cisco Nexus 1000V. El conmutador virtual aporta la potencia de un conmutador Cisco al entorno de red virtualizado.



2.1.2 Tipos de Nubes

Los cuatro modelos principales en la nube son:

- **Nubes Públicas** - Las aplicaciones basadas en la nube y los servicios que se ofrecen en una nube pública están a disposición de la población en general. Los servicios pueden ser gratuitos u ofrecerse sobre la base de pago por utilización, como el pago por almacenamiento en línea. La nube pública utiliza Internet para proporcionar servicios.
- **Nubes Privadas** - Las aplicaciones y los servicios basados en una nube privada que se ofrecen en la misma están destinados a una organización o una entidad específica, como el gobierno. Se puede configurar una nube privada usando la red privada de una organización, aunque esto puede ser costoso de construir y mantener. Una nube privada también puede ser administrada por una organización externa con estricta seguridad de acceso.
- **Nubes Híbridas** - Una nube híbrida consta de dos o más nubes (por ejemplo, una parte privada y otra parte pública), donde cada una de las partes sigue siendo un objeto separado, pero ambas están conectadas a través de una única arquitectura. En una nube híbrida, las personas podrían tener grados de acceso a varios servicios según sus derechos de acceso de usuario.
- **Nubes Comunitarias** - Una nube comunitaria se crea para el uso exclusivo de una comunidad específica. Las diferencias entre nubes públicas y nubes comunitarias son las necesidades funcionales que se personalizan para la comunidad. Por ejemplo, las organizaciones de servicios de salud deben cumplir las políticas y leyes (p. ej., HIPAA, en los Estados Unidos) que requieren niveles de autenticación y confidencialidad especiales.

2.1.3 Computación en la Nube y Virtualización

Los términos “computación en la nube” y “virtualización” a menudo se usan indistintamente; sin embargo, significan cosas diferentes. La virtualización es la base de la computación en la nube. Sin ella, la computación en la nube, como se implementa más ampliamente, no sería posible.

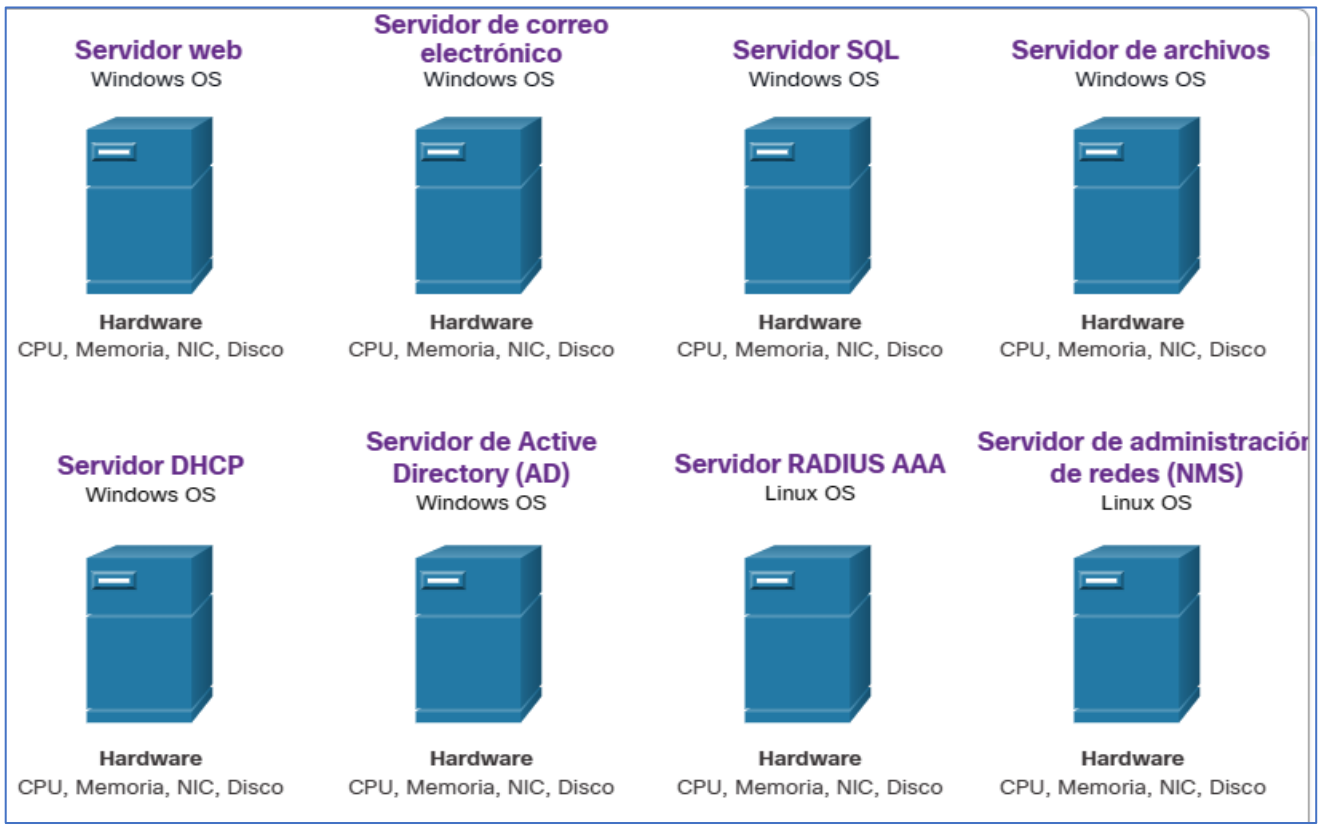
Hace más de una década, VMware desarrolló una tecnología de virtualización que permitía que un sistema operativo host admitiera uno o más sistemas operativos cliente. La mayoría de las tecnologías de virtualización ahora se basan en esta tecnología. La transformación de servidores dedicados a servidores virtualizados ha sido adoptada y se está implementando rápidamente en centros de datos y redes empresariales.

La virtualización significa crear una versión virtual en lugar de física de algo, como una computadora. Un ejemplo sería ejecutar una "computadora Linux" en su PC con Windows, lo que hará más adelante en el laboratorio.

Para apreciar completamente la virtualización, primero es necesario comprender algo de la historia de la tecnología de servidores. Históricamente, los servidores empresariales consistían en un sistema operativo de servidor, como Windows Server o Linux Server, instalado en un hardware

específico, como se muestra en la figura. Toda la RAM del servidor, la potencia de procesamiento y el espacio del disco duro se dedicaban al servicio prestado (por ejemplo, servicios web, de correo electrónico, etc.)

El principal problema con esta configuración es que cuando falla un componente, el servicio proporcionado por este servidor no se encuentra disponible. Esto se conoce como punto único de falla. Otro problema era que los servidores dedicados eran infrautilizados. A menudo, los servidores dedicados estaban inactivos durante largos períodos de tiempo, esperando hasta que hubiera una necesidad de ofrecer un servicio específico que estos proporcionaban. Estos servidores malgastaban energía y ocupaban más espacio del que estaba garantizado por la cantidad de servicio. Esto se conoce como proliferación de servidores.



2.1.4 Verifique su comprensión - La Nube y Servicios en la Nube

¿Qué modelo de nube representa dos o más nubes donde cada parte sigue siendo un objeto distintivo, pero ambas están conectadas usando una sola arquitectura?

Nube publica	Nube privada	Nube hibrida ☺←	Nube comunitaria

El modelo de nube híbrida representa dos o más nubes donde cada parte sigue siendo un objeto distintivo, pero ambas están conectadas usando una sola arquitectura.

¿Qué modelo de nube se usa para satisfacer las necesidades de una industria específica, como la atención médica o los medios de comunicación?

Nube publica	Nube privada	Nube hibrida	Nube comunitaria ☺←

El modelo de nube comunitaria se utiliza para satisfacer las necesidades de una industria específica, como la atención médica o los medios de comunicación.

¿Qué dispositivo utiliza toda la RAM, la potencia de procesamiento y el espacio del disco duro dedicado a un servicio?

Servidor dedicado ☺←	Dispositivo móvil	Máquina virtual	Servidor virtualizado

Un servidor dedicado utiliza toda la RAM, la potencia de procesamiento y el espacio en el disco duro dedicado a un servicio.

2. Virtualización

2.2.1 Ventajas de la Virtualización

Una de las ventajas más importantes de la virtualización es un menor costo total:

- **Se requiere menos equipo** - La virtualización permite la consolidación de servidores, lo que requiere menos dispositivos físicos y reduce los costos de mantenimiento.
- **Menor consumo de energía** - La consolidación de servidores reduce los costos mensuales de alimentación y refrigeración.
- **Se requiere menos espacio** - La consolidación de servidores reduce la cantidad de espacio requerido.

Estos son los beneficios adicionales de la virtualización:

- **Simplificación de prototipos** - Se pueden crear rápidamente laboratorios autónomos que operan en redes aisladas para las pruebas y los prototipos de instalaciones de red.
- **Aprovisionamiento más rápido de servidores** - La creación de un servidor virtual es mucho más rápida que el aprovisionamiento de un servidor físico.
- **Mayor tiempo de actividad del servidor** - La mayoría de las plataformas de virtualización de servidores ahora ofrecen funciones avanzadas redundantes de tolerancia a fallas.
- **Recuperación mejorada ante desastres** - La mayoría de las plataformas de virtualización de servidores empresariales tienen software que puede ayudar a probar y automatizar la conmutación por error antes de que ocurra un desastre.
- **Soporte de tecnologías heredadas** - La virtualización puede extender la vida útil de los sistemas operativos y las aplicaciones, brindando más tiempo para que las organizaciones migren a soluciones más nuevas.

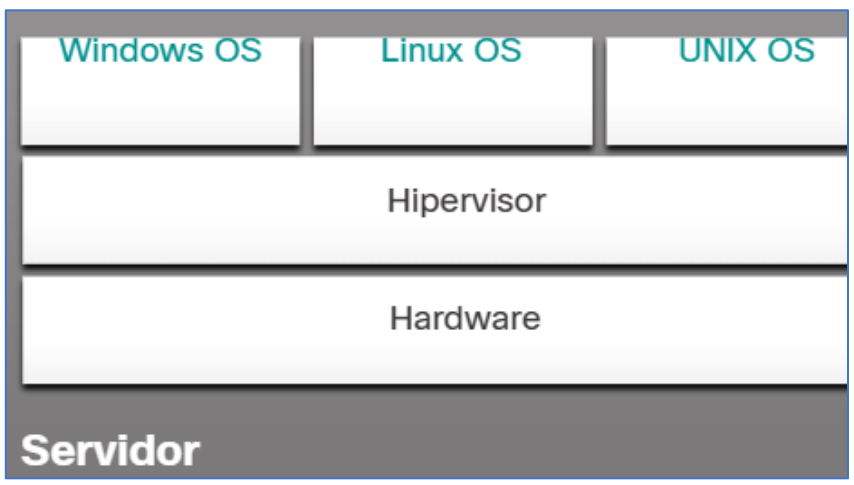
2.2.2 Hipervisores

El Hipervisor es un programa, un firmware o un hardware que suma una capa de abstracción a la parte superior del hardware físico real. La capa de abstracción se utiliza para crear máquinas virtuales que tienen acceso a todo el hardware de la máquina física, como CPU, memoria, controladores de disco y NIC. Cada una de esas máquinas virtuales ejecuta un sistema operativo completo y separado. Con la virtualización, no es raro que 100 servidores físicos se consoliden como máquinas virtuales sobre 10 servidores físicos que usan hipervisores.

Hipervisor Tipo 1 - Enfoque de Infraestructura Física (Bare Metal)

El hipervisor de tipo 1 también se denomina infraestructura física (Bare metal), porque el hipervisor está instalado directamente en el hardware. Los hipervisores de tipo 1 se usan generalmente en los servidores empresariales y los dispositivos de redes para centros de datos.

Con los hipervisores de tipo 1, el hipervisor se instala directamente en el servidor o en el hardware de red. Luego, las instancias de OS se instalan sobre el hipervisor, como se muestra en la figura. Los hipervisores de tipo 1 tienen acceso directo a los recursos de hardware; por lo tanto, son más eficaces que las arquitecturas alojadas. Los hipervisores de tipo 1 mejoran la escalabilidad, el rendimiento y la solidez.



Hipervisor Tipo 2 – Enfoque “alojado”

Un hipervisor, tipo 2, es un software que crea y ejecuta instancias de VM. La computadora en la que un hipervisor está ejecutando una o más VM, es un equipo host. Los hipervisores de tipo 2 también se denominan hipervisores alojados. Esto se debe a que el hipervisor está instalado sobre el OS existente, como Mac OS X, Windows o Linux. Luego, una o más instancias adicionales de OS se instalan sobre el hipervisor, como se muestra en la figura. Una gran ventaja de los hipervisores de tipo 2 es que no es necesario el software de consola de administración.

Nota: Es importante asegurarse de que la máquina de host sea lo suficientemente robusta como para instalar y ejecutar las VM, a fin de evitar que se agoten los recursos.

2.2.3 Laboratorio - Instalar de Linux en una Máquina Virtual y Explorar la GUI

En esta práctica de laboratorio, instalará el sistema operativo Linux en una máquina virtual mediante una aplicación de virtualización de equipos de escritorio, como VirtualBox. Después de completar la instalación, explorará la interfaz de la GUI.

Práctica de laboratorio - instalación de Linux en una máquina virtual y exploración de la GUI

Objetivos

- Parte 1: Preparar una computadora para la virtualización
- Parte 2: Instalar un sistema operativo Linux en la máquina virtual
- Parte 3: Explorar la interfaz gráfica de usuario

Aspectos básicos/Situación

El poder computacional y los recursos, han aumentado enormemente en los últimos 10 años. Una ventaja de los procesadores multinúcleo y las grandes cantidades de memoria RAM es la capacidad de instalar varios sistemas operativos a través del uso de la virtualización en una computadora.

Con la virtualización, una o más computadoras virtuales pueden operar dentro de una computadora física. Las computadoras virtuales que se ejecutan dentro de computadoras físicas se denominan "máquinas virtuales”. Las máquinas virtuales se conocen como “guests (invitados)” y las computadoras físicas se conocen como “hosts (huéspedes)”. Cualquier persona con una computadora y sistema operativo modernos puede ejecutar máquinas virtuales.

En esta práctica de laboratorio, instalará el sistema operativo Linux en una máquina virtual mediante una aplicación de virtualización de equipos de escritorio, como VirtualBox. Después de completar la instalación, explorará la interfaz de la GUI. También explorará la interfaz de línea de comandos usando esta máquina virtual en una práctica de laboratorio posterior en este curso.

Recursos necesarios

- Computadora con un mínimo de 2 Gb de RAM y 10 Gb de espacio libre en disco
- Acceso a Internet de alta velocidad para descargar imágenes de VirtualBox de Oracle y del sistema operativo Linux, como Ubuntu Desktop

Instrucciones

PARTE 1: Preparar una computadora para la virtualización

Descargará e instalará software de virtualización de equipos de escritorio y una imagen del sistema operativo Linux. El instructor puede proporcionarle una imagen del sistema operativo Linux.

Paso 1: Descargar e instalar VirtualBox.

VMware Player y Oracle VirtualBox son dos programas de virtualización que puede descargar e instalar para admitir el archivo de imagen del sistema operativo. En esta práctica de laboratorio, usará la aplicación VirtualBox.

a) Navegue hasta https://www.VirtualBox.org Haga clic en el enlace de descarga en esta página.
b) Elija y descargue el archivo de instalación adecuado según su sistema operativo.
c) Cuando se haya descargado el archivo de VirtualBox, ejecute el instalador y acepte la configuración de instalación predeterminada.

Paso 2: Descargar una imagen de Linux

a. Navegue hasta el sitio web de Ubuntu en http://www.Ubuntu.com. Haga clic en el enlace de descarga en esta página para descargar y guardar una imagen de Ubuntu Desktop.

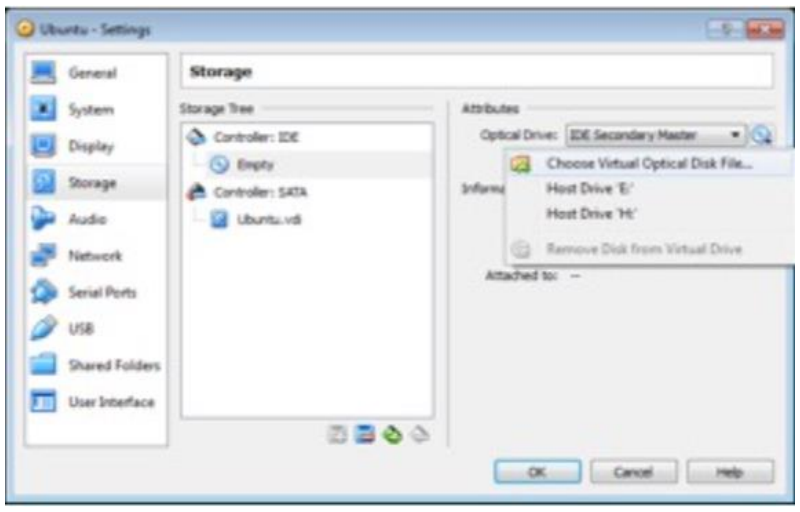
Paso 3: Crear una máquina virtual nueva

a. Haga clic en Inicio y busque VirtualBox. Haga clic en Oracle VM VirtualBox para abrir el administrador. Cuando se abra, haga clic en Nuevo para comenzar la instalación de Ubuntu.
b. En la pantalla Nombre y sistema operativo, escriba Ubuntu en el campo Nombre. En el campo Tipo, seleccione Linux. En el campo Versión, seleccione la versión descargada correspondiente. Haga clic en Siguiente para continuar.
c. En la pantalla Tamaño de memoria, aumente la cantidad de RAM teniendo en cuenta que la memoria de la máquina virtual siempre debe estar en el área verde. Si se excede el área verde, tendrá un efecto adverso en el rendimiento del host Haga clic en Siguiente para continuar.
d. En la pantalla Unidad de disco duro, haga clic en Crear para crear ahora un disco duro virtual.
e. En la pantalla Tipo de archivo de unidad de disco duro, utilice las configuraciones de tipo de archivo predeterminado de VDI (imagen de disco de VirtualBox). Haga clic en Siguiente para continuar.
f. En la pantalla Almacenamiento en unidad de disco duro físico, utilice las configuraciones predeterminadas de almacenamiento de asignación dinámica. Haga clic en Siguiente para continuar.
g. En la pantalla Ubicación y tamaño del archivo, puede ajustar la unidad de disco duro y cambiar el nombre y la ubicación del disco duro virtual. Haga clic en Crear para usar la configuración predeterminada.
h. Una vez que se creó la unidad de disco duro, la máquina virtual nueva aparece en una lista en la ventana Oracle VM VirtualBox Administrador. Seleccione Ubuntu y haga clic en Iniciar en el menú superior.

PARTE 2: Instalar Ubuntu en la máquina virtual

Paso 1: Monte la imagen.

a. En la ventana Administrador de Oracle VM VirtualBox, Haga clic con el botón secundario del mouse en Ubuntu y seleccione Configuración. En la ventana Ubuntu – Configuración, haga clic en Almacenamiento en el panel izquierdo. Haga clic en Vacío en el panel central. En el panel derecho, haga clic en el símbolo de CD y seleccione la ubicación de la imagen de Ubuntu. Haga clic en Aceptar para continuar.
b. En la ventana Administrador de Oracle VM VirtualBox, haga clic en Iniciar en el menú superior.



Paso 2: Instale el sistema operativo.

a. En la pantalla **Bienvenido**, se le solicitará que pruebe o instale Ubuntu. La opción de prueba no instala el sistema operativo, sino que lo ejecuta directamente desde la imagen. En esta práctica de laboratorio, instalará el sistema operativo de Ubuntu en esta máquina virtual. Haga clic en **Instalar Ubuntu**.

b. Siga las instrucciones en pantalla y proporcione la información necesaria cuando se le solicite.

Nota: Si no está conectado a Internet, puede continuar con la instalación y habilitar una red más adelante.

c. Dado que esta instalación de Ubuntu está en una máquina virtual, es seguro borrar el disco e instalar Ubuntu sin afectar al equipo host. Seleccione **Borrar disco e instalar Ubuntu**. Caso contrario, la instalación de Ubuntu en una computadora física borraría todos los datos del disco y reemplazaría el sistema operativo existente con Ubuntu. Haga clic en **Instalar** ahora para comenzar la instalación.

d. Haga clic en **Continuar** para borrar el disco e instalar Ubuntu.

e. En la pantalla **¿Quién es usted?**, proporcione su nombre y elija una contraseña. Puede utilizar el nombre de usuario generado o ingresar un nombre de usuario diferente. Escriba su nombre de usuario y contraseña. Si lo desea, puede cambiar los otros parámetros. Haga clic en **Continuar**.

f. El sistema operativo Ubuntu ahora está instalando en la máquina virtual. Esto puede tardar varios minutos. Cuando aparezca el mensaje **Se completó la instalación**, vuelva a la ventana **Administrador de Oracle VM VirtualBox**. Haga clic con el botón secundario del mouse en **Ubuntu** y seleccione **Configuración**. En la ventana **Ubuntu – Configuración**, haga clic en **Almacenamiento** en el panel izquierdo. Haga clic en la imagen montada de Ubuntu en el panel central. En el panel derecho, haga clic en el símbolo de CD y, luego, en **Quitar disco de la unidad virtual**. Haga clic en **Aceptar** para continuar.

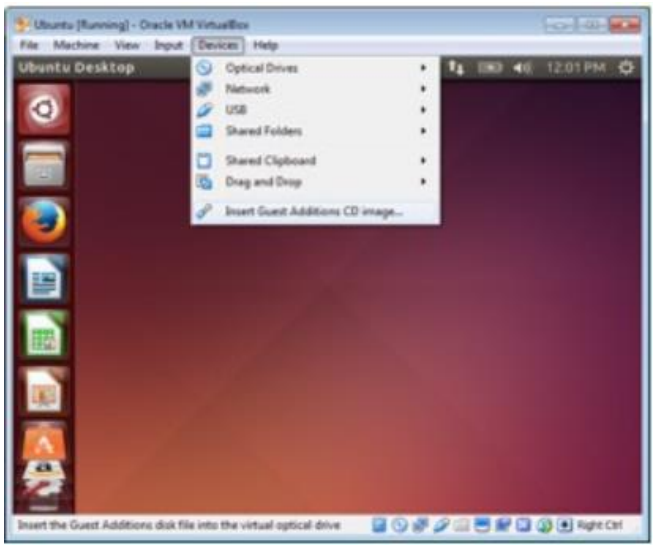
g. En la VM de Ubuntu, haga clic en **Reiniciar ahora**.

PARTE 3: Explorar la interfaz gráfica de usuario

En esta parte, instalará las Guest Additions de VirtualBox y explorará la interfaz gráfica de usuario (GUI) de Ubuntu.

Paso 1: Instalar Guest Additions

a. Inicie sesión en su máquina virtual con Ubuntu utilizando las credenciales de usuario que creó en la parte anterior.
b. La ventana del escritorio de Ubuntu puede ser más pequeña que lo esperado. Esto sucede, en particular, con las pantallas de alta resolución. Haga clic en Dispositivo > Insertar imagen de CD de Guest Additions… para instalar las Guest Additions. Esto permite que haya más funciones, como cambiar la resolución de pantalla de la máquina virtual.



c. Haga clic en **Ejecutar** para instalarlas. Cuando se le solicite una contraseña, utilice la misma que usó para iniciar sesión. Haga clic en **Autenticar** para continuar.
d. Si la computadora no estaba conecta a Internet durante la instalación, haga clic en **Dispositivos > Configuración** de red en el menú de Oracle VirtualBox. Habilite los adaptadores de red y configure la configuración adecuada para las conexiones de red, según sea necesario. Haga clic en **Aceptar**.
e. Cuando se complete la instalación del paquete Guest Additions, vuelva a reiniciar la máquina virtual. Haga clic en el menú del ángulo superior derecho y en **Cerrar**. Haga clic en **Reiniciar** para reiniciar Ubuntu.

Paso 2: Abrir un navegador web

a. Vuelva a iniciar sesión en Ubuntu. Una vez que haya iniciado sesión, puede cambiar el tamaño de la ventana de la máquina virtual.
b. Abra un navegador web Según la distribución de Linux, es posible que deba buscar un navegador web o que ya haya un enlace a un navegador web en el escritorio.
c. Busque un emulador de terminal para acceder a la interfaz de línea de comandos. Utilizará un emulador de terminal en prácticas de laboratorio posteriores.
d. Explore la distribución instalada de Linux y busque algunas aplicaciones que puede utilizar.

Pregunta de reflexión

¿Cuáles son las ventajas y desventajas de usar una máquina virtual?

Con una máquina virtual, puede probar aplicaciones o sistemas operativos nuevos sin afectar su equipo host. También puede guardar el estado actual de la máquina cuando cierra la máquina virtual. Si tiene problemas, tiene la opción de regresar la máquina virtual a un estado previamente guardado. Por otro lado, una máquina virtual requiere los recursos de hardware del equipo host, como espacio en el disco duro, memoria RAM y potencia de procesamiento.

3. Resumen de la nube y virtualización

2.3.1 ¿Qué Aprendí en este Módulo?

La nube y servicios en la nube

Generalmente cuando hablamos de la nube, hablamos de tres elementos: centros de datos, computación en la nube y virtualización. Los centros de datos suelen ser grandes instalaciones que proporcionan grandes cantidades de energía, refrigeración y ancho de banda. Solo empresas muy grandes pueden permitirse sus propios centros de datos. La mayoría de las organizaciones más pequeñas arrienda los servicios de un proveedor de la nube.

Los servicios en la nube incluyen lo siguiente:

- SaaS - Software como servicio
- PaaS - Plataforma como servicio
- IaaS - Infraestructura como servicio.

Hay cuatro modelos de nube principales:

1. Nubes Públicas - Las aplicaciones basadas en la nube y los servicios que se ofrecen en una nube pública están a disposición de la población en general.
2. Nubes Privadas - Las aplicaciones y los servicios basados en una nube privada que se ofrecen en una nube privada están destinados a una organización o una entidad específica, como el gobierno.
3. Nubes híbridas - Una nube híbrida se compone de dos o más nubes, donde cada parte sigue siendo un objeto separado, pero ambas están conectadas mediante una única arquitectura.
4. Nubes Comunitarias - Una nube comunitaria se crea para el uso exclusivo de una comunidad específica. Las diferencias entre nubes públicas y nubes comunitarias son las necesidades funcionales que se personalizan para la comunidad.

La virtualización es la base de la computación en la nube. Sin esta base, la computación en la nube que se implementa masivamente no sería posible. La virtualización significa crear una versión virtual un lugar de una versión física de algo, como una computadora. Un ejemplo sería ejecutar una “computadora con Linux” en su PC con Windows.

Virtualización

Una de las ventajas más importantes de la virtualización es un menor costo total:

- Se requiere menos equipo - La virtualización permite la consolidación de servidores, lo que requiere menos dispositivos físicos y reduce los costos de mantenimiento.
- Menor consumo de energía - La consolidación de servidores reduce los costos mensuales de alimentación y refrigeración.
- Se requiere menos espacio - La consolidación de servidores reduce la cantidad de espacio requerido.

Estos son los beneficios adicionales de la virtualización:

- Simplificación de prototipos - Se pueden crear rápidamente laboratorios autónomos operando en redes aisladas para poner a prueba los prototipos de instalaciones de red.
- Aprovisionamiento de servidores más rápido - Crear un servidor virtual es mucho más rápido que aprovisionar un servidor físico.
- Mayor tiempo de actividad del servidor - La mayoría de las plataformas de virtualización de servidores ahora ofrecen funciones avanzadas de tolerancia a fallas redundantes.
- Recuperación mejorada ante desastres - La mayoría de las plataformas de virtualización de servidores empresariales tienen software que automatizan la conmutación por errores antes de que ocurra un desastre.
- Soporte de tecnologías heredadas - La virtualización puede extender la vida útil de los sistemas operativos y las aplicaciones, brindando más tiempo para que las organizaciones migren a soluciones más nuevas.

El Hipervisor es un programa, un firmware o un hardware que suma una capa de abstracción a la parte superior del hardware físico real. La capa de abstracción se utiliza para crear máquinas virtuales que tienen acceso a todo el hardware de la máquina física, como CPU, memoria, controladores de disco y NIC. Cada una de esas máquinas virtuales ejecuta un sistema operativo completo y separado.

El hipervisor de tipo 1 también se denomina infraestructura física (Bare metal), porque el hipervisor está instalado directamente en el hardware. Los hipervisores de tipo 1 se usan generalmente en Servidores Empresariales y en dispositivos de redes para Centros de Datos.

Un hipervisor, tipo 2, es un software que crea y ejecuta instancias de VM. La computadora, en la que un hipervisor está ejecutando una o más VM, es un equipo host. Los hipervisores de tipo 2 también se denominan hipervisores alojados. Esto se debe a que el hipervisor está instalado sobre el OS existente, como Mac OS X, Windows o Linux. Luego, una o más instancias adicionales de OS se instalan sobre el hipervisor. Una gran ventaja de los hipervisores de tipo 2 es que el software de la consola de administración no es necesario.

2.3.2 Webster - Preguntas de Reflexión

Por ahora, Bob sugiere que Marcy y Vincent utilicen la nube para el almacenamiento de datos. Entienden que es un servicio de suscripción, pero les permitirá mantener sus datos de manera más segura y será menos costoso que comprar su propio servidor y almacenamiento de datos. Como ya sabe, la nube ofrece muchos otros servicios. Es posible que Marcy y Vincent finalmente deseen algunos de estos servicios también. ¿Alguna vez le pasó que su disco duro dejó de funcionar y no puede recuperar todos sus archivos? ¿Qué pasaría si esto le sucediera a una computadora o incluso a un servidor en tu escuela o trabajo? ¿La red de su escuela o trabajo utiliza otros servicios en la nube? Si es así, ¿sabe cuáles son y por qué se seleccionaron? Si estuviera en la situación de Marcy y Vincent, ¿qué servicios en la nube consideraría usar además del almacenamiento de datos?

2.3.3 Prueba de La Nube y Virtualización

¿Qué término se asocia con la computación en la nube?

Trabajadores a distancia	Inalámbrica	Servidores altos	Virtualización ☺←

¿Cuáles tres características representan los beneficios de la virtualización? (Escoja tres opciones)

Menor consumo de energía ☺←	Menos capacitación técnica de los empleados	Menor monitoreo de los dispositivos
Menos equipos ☺←	Mejor recuperación tras un desastre ☺←	Menos requisitos de seguridad

¿Qué modelo de nube proporciona servicios para una organización o entidad específica?

Hibrida	Comunitaria	Publica	Privada ☺←

¿Qué término describe el tipo de servicio de computación en la nube que proporciona aplicaciones en la web?

IaaS	ITaaS	PaaS	SaaS ☺←

Guardar sus fotos en una ubicación de almacenamiento mantenida por su proveedor de servicios es un ejemplo de

Virtualización	Datos masivos	Computación en la nube ☺←

Una empresa utiliza los servicios en la nube y está configurando un nuevo switch suministrado por el proveedor de la nube. ¿Qué modelo de nube utiliza la compañía?

DaaS	IaaS ☺←	PaaS	SaaS ☺←

¿Qué término se utiliza para definir el proceso de software que crea VM y realiza la abstracción de hardware para admitir VM?

Hipervisor ☺←	Contenedor	Administrador de elementos	Administrador de infraestructura virtualizada (VIM)

¿Qué tipo de nube consta de dos o más nubes conectadas a través de una sola arquitectura?

Hibrida ☺←	Comunitaria	Publica	Privada

¿Cuáles son los dos hipervisores tipo 2? (Elija dos opciones).

VirtualBox ☺←	VMware ESXi	Xen	Virtual PC ☺←	KVM

¿Qué es una característica de una nube pública?

Disponible para todos ☺←	Destinada a una organización específica	Formada por dos o más nubes	Personalizada para necesidades específicas de las organizaciones

Consultar la ilustración. ¿Qué tipo de software se instala en el sistema host para admitir las tres máquinas virtuales?

- ✓ Hipervisor de tipo 2
- software bare metal
- Hipervisor de tipo 1
- software de computación de perímetro

Módulo 3: Sistemas de Numeración

0. Introducción

3.0.1 Webster - ¿Por Qué Debería Tomar este Módulo?

¡Webster aquí otra vez! Bob es bueno en esto de las redes. Cuando aprendió sobre redes, tenía que entender los sistemas de números, ¡y usted también! Ya utiliza el sistema decimal de base 10, que utiliza los enteros 0-9. ¿Conoce otros sistemas numéricos? He visto base-12, base-60 y otros. ¿Conoce el sistema binario que usan las computadoras? El sistema binario utiliza solo dos enteros, 0 y 1. Los hosts, los servidores y los dispositivos de red utilizan direccionamiento binario. También hay algo llamado sistema de numeración hexadecimal. Se usa en redes para representar direcciones IP Versión 6 y direcciones MAC Ethernet.

¡Aproveche este módulo para obtener más información sobre estos sistemas numéricos y cómo convertirlos!

3.0.2 ¿Qué Aprenderé en este Módulo?

Título del Módulo: Sistemas Numéricos

Objetivo del Módulo: Calcular números entre los sistemas decimal, binario y hexadecimal.

Título del Tema	Objetivo del Tema
Sistema Numérico Binario	Calcule los números entre los sistemas decimales y binarios.
Sistema Numérico Hexadecimal	Calcule los números entre los sistemas decimales y hexadecimales.

1. Sistema numérico binario

3.1.1 Direcciones Binarias e IPv4

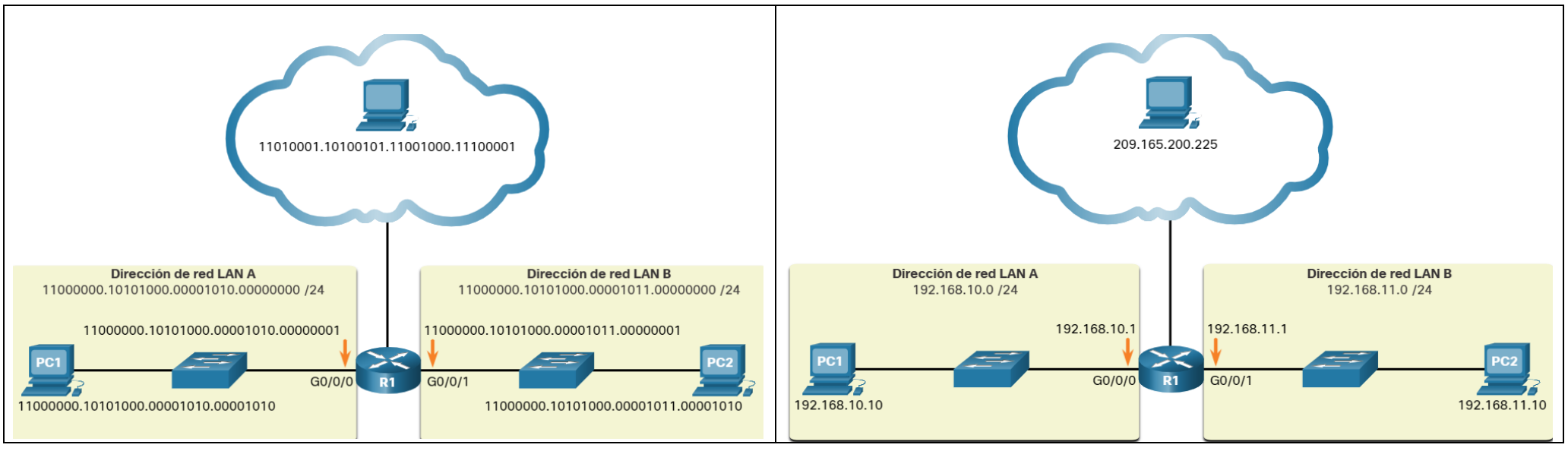
Las direcciones IPv4 comienzan como binarias, una serie de solo 1s y 0s. Estos son difíciles de administrar, por lo que los administradores de red deben convertirlos a decimales. En este tema se muestran algunas formas de hacerlo. Binario es un sistema de numeración que consta de los dígitos 0 y 1 llamados bits. Por el contrario, el sistema de numeración decimal consta de 10 dígitos que incluye del 0 al 9.

Es importante que comprendamos el sistema binario, ya que los hosts, los servidores y los dispositivos de red usan el direccionamiento binario. Específicamente, usan direcciones IPv4 binarias, como se muestra en la figura 1, para identificarse entre sí.

Cada dirección consta de una cadena de 32 bits, divididos en cuatro secciones denominadas octetos. Cada octeto contiene 8 bits (o 1 byte) separados por un punto. Por ejemplo, a la PC1 de la ilustración se le asignó la dirección IPv4 11000000.10101000.00001010.00001010.

La dirección de gateway predeterminado sería la de la interfaz Gigabit Ethernet G0/0/0 del R1, 11000000.10101000.00001010.00000001. El binario funciona bien con hosts y dispositivos de red. Sin embargo, es muy difícil para los humanos trabajar con él. Para facilitar el uso por parte de las personas, las direcciones IPv4 se expresan comúnmente en notación decimal punteada. A la PC1 se le asigna la dirección IPv4 192.168.10.10, y su dirección de puerta de enlace predeterminada es 192.168.10.1, como se muestra en la figura 2.

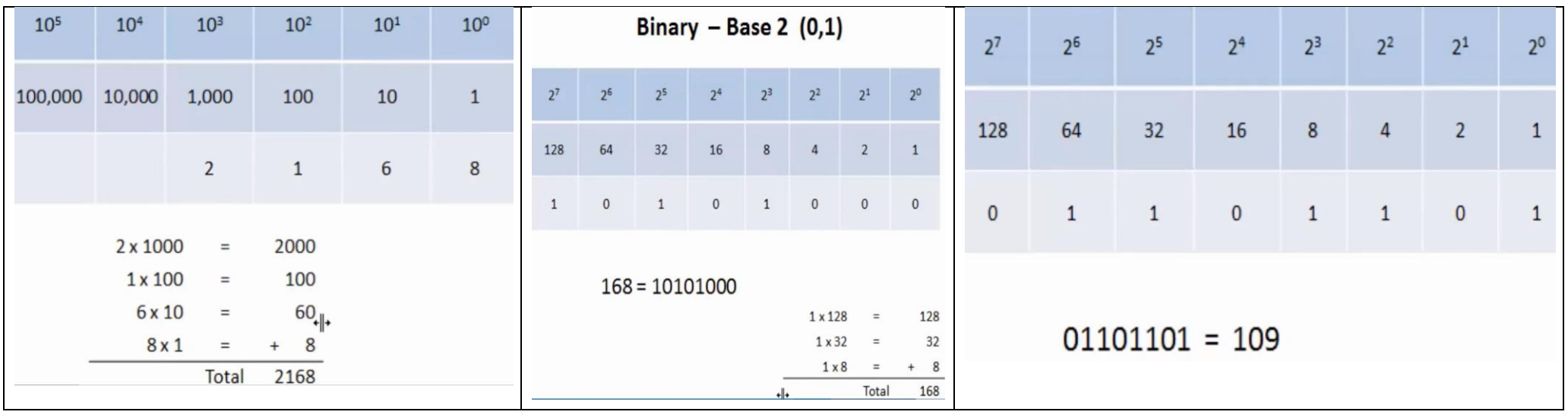
Para tener una buena comprensión del direccionamiento de red, es necesario comprender el direccionamiento binario y obtener habilidades prácticas en la conversión entre direcciones IPv4 binarias y direcciones decimales punteadas. Esta sección cubrirá cómo convertir entre sistemas de numeración de base dos (binario) y base 10 (decimal).



3.1.2 Video - Conversión Entre Sistemas de Numeración Binarios y Decimales

En este video, voy a hablar sobre la conversión de binario a decimal, pero antes de hacerlo, quiero echar un vistazo a la notación posicional o los valores de lugar. Aquí tengo el número 2168. Si miramos los valores posicionales del número 2168, concebimos que los valores posicionales tienen las unidades, las decenas, las centenas, los miles, los 10,100 mil y los millones. Estos son los valores posicionales del sistema numérico decimal de base 10. Puedes ver que tenemos el número dos en los mil. Así que tenemos dos mil, tenemos uno en el lugar de las centenas para

100, tenemos seis en el lugar de los 10 para 60 y tenemos ocho en el lugar de las unidades para ocho. Así que efectivamente tenemos dos unidades de mil, una de 100 6 decenas de 60 y ocho unidades de 8. Ahora, cuando hablamos de los valores posicionales en el sistema numérico decimal, estamos hablando de las potencias de 10. Puedes ver que el lugar de las unidades es 10 elevado a cero. El lugar de 10 es 10 elevado a uno, el lugar de las centenas 10 elevado a dos, o 10 * 10, que es 100. El lugar de los miles es el 10 elevado a tres, o 10 * 10 * 10 y así sucesivamente y así sucesivamente. Así que puedes ver que los valores posicionales se basan en potencias de 10. Si miramos el número 2168, entonces en forma larga podemos ver que efectivamente tenemos dos mil. Uno 100. Seis 10 y ocho unos y 2000 + 100 + 60 + 8 suman 2168. Este es el tipo de conteo y suma que aprendemos de niños. El sistema decimal. Es base 10. Se basa en el hecho de que tienes una potencia de 10, pero lo más importante es que tienes 10 caracteres o 10 números en este sistema de conteo desde cero hasta el 9. Eso significa que en cada valor posicional puedes tener desde el 0 hasta el 9, en otras palabras. Si tuviera el número 9168, yo simplemente reemplacé los dos aquí con 9 y ahora tengo 9 Mil, totalizando 9000. Entonces, en cualquiera de estos valores de posición puede tener el número 0 hasta el 9. Este es el sistema de numeración decimal base 10. Si consideramos binario y lo miramos de la misma manera que decimal. Binario es un sistema numérico de base dos. Solo hay dos caracteres o dos números, cero y uno. Así que bajo los valores posicionales solo podemos tener 0s o 1s. Los valores posicionales van del 1, que es 2^0, 2 que es 2^1, 4 que es 2^2, 8 que es 2^3, hasta 128 que es 2^7. Observe que amplié la tabla a ocho valores posicionales. Eso es porque ocho bits es una agrupación importante de números, 8 bits forman un byte en el procesamiento informático. Así que ahora tengo los valores posicionales para esencialmente 8 bits. Si quiero escribir el número 168 en binario, solo tengo que encontrar los valores de lugar correspondientes y conectar 1 o 0. Así que iré al lugar 128 y me preguntaré, ¿necesito 128 para llegar a 168? Sí, así que pondré uno allí. ¿Ahora necesito un 64? Ya tengo un 128. Si sumo 64 obtendría 192 porque 128 + 64 es 192. Entonces la respuesta es no. Así que puse un 0. Tengo 128 ahora. ¿Necesito un 32? 128 + 32 es 160. Así que sí, pongo 1 aquí. Ahora tengo 160. ¿Necesito un 16? No. Eso haría 176, lo que superaría mi objetivo de 168. Pondré un cero aquí. ¿Qué tal un 8? Si sumo un 8, acertaré el número perfectamente. 128 + 32 + 8 es 168. Seguiré con ceros en el lugar del 4, en el lugar de 2, y el lugar de las unidades. Y 168 en binario es igual a 10101000. Ahora tengo 128+32+8=168. Si pasamos a la siguiente diapositiva, ahora puede ver que estoy a cargo de convertir el número 01101101 a decimal. Si quiero ir en sentido contrario, convierta este número binario a decimal, todo lo que necesito hacer es insertarlo en los valores posicionales. Lo pondré aquí 0.1.1.0.1.1.01 y luego lo sumaré. Tengo un 64. Y tengo un 32, 64 + 32 es 96. Además, tengo un 8 que da 104. Más cuatro hacen 108 + 1 da 109. Este número convertido a decimal es el número 109. Ahora veamos una dirección IP completa en binario. Pasaré a la siguiente diapositiva. En la siguiente diapositiva, puede ver que ahora tengo una dirección IP de 32 bits, 11000000.10101000.00000001.01100101 4 octetos o 32 bits en total. Si quiero convertir esta dirección IP binaria a decimal, todo lo que necesito hacer es contar cada octeto individual. Comencemos con el primero aquí. Podemos ver que 128 + 64 es 192. Ahora el próximo octeto 128+32+8=168. El siguiente octeto es todo ceros con un uno en el último lugar en el lugar de las unidades, es el número 1. Y finalmente tenemos el ultimo octeto 64+32+4+1=101. Entonces, la conversión de esta dirección IP binaria a decimal es 192.168.1.101.



3.1.3 Verifique su Comprensión - Sistema Numérico Binario

¿Cuál es el binario equivalente a la dirección IP 192.168.11.10?

- 11000000.11000000.00001011.00001010
- ✓ 11000000.10101000.00001011.00001010
- 11000000.10101000.00001010.00001011
- 11000000.10101000.00001011.00010010

¿Cuál de los siguientes es el binario equivalente a la dirección IP 172.16.31.30?

- 11000000.00010000.00011111.00011110
- 10101000.00010000.00011111.00011110
- 10101100.00010000.00011110.00011110
- ✓ 10101100.00010000.00011111.00011110

3.1.4 Actividad - Conversión de Binario a Decimal

Instrucciones

Esta actividad le permite practicar la conversión de binario a decimal de 8 bits tanto como sea necesario. Le recomendamos que trabaje con esta herramienta hasta que pueda realizar la conversión sin errores. Convierta el número binario que se muestra en el octeto a su valor decimal.

Valor decimal	159							
Base	2	2	2	2	2	2	2	2
Exponente	7	6	5	4	3	2	1	0
Posición	128	64	32	16	8	4	2	1
Bit	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**1**

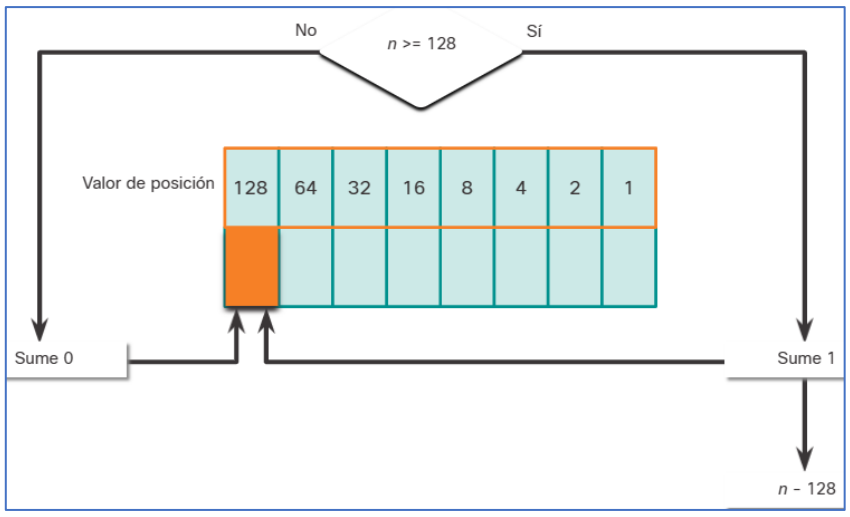
3.1.5 Conversión de Decimal a Binario

También es necesario comprender cómo convertir una dirección IPv4 decimal punteada a una binaria. La tabla de valores de posición binarios es una herramienta útil. Haga clic en cada posición a partir de 128 y trabaje su camino de izquierda a derecha a la posición 1.

128

¿Es el número decimal del octeto (n) igual o mayor que el bit más significativo (128)?

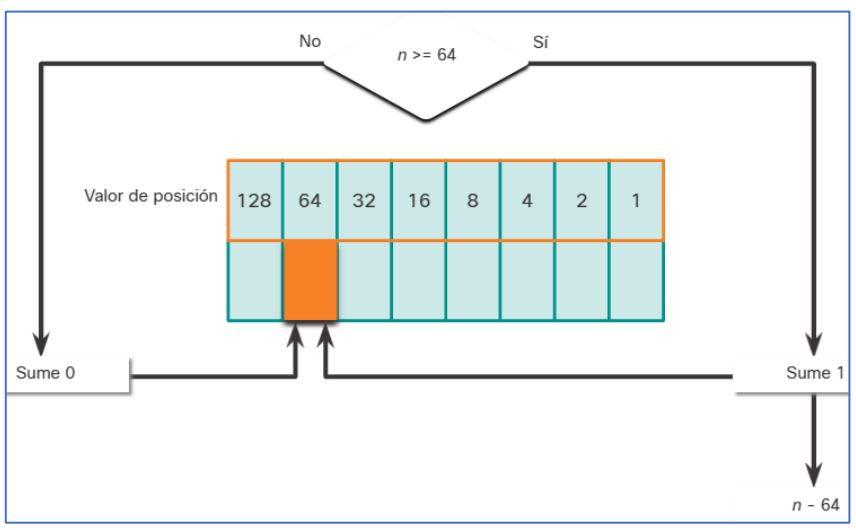
- Si no es así, introduzca un valor binario 0 en el valor de posición 128.
- Si es así, agregue un valor binario 1 al valor de posición 128 y reste 128 del número decimal.



64

¿Es el número decimal del octeto (n) igual o mayor que el siguiente bit más significativo (**64**)?

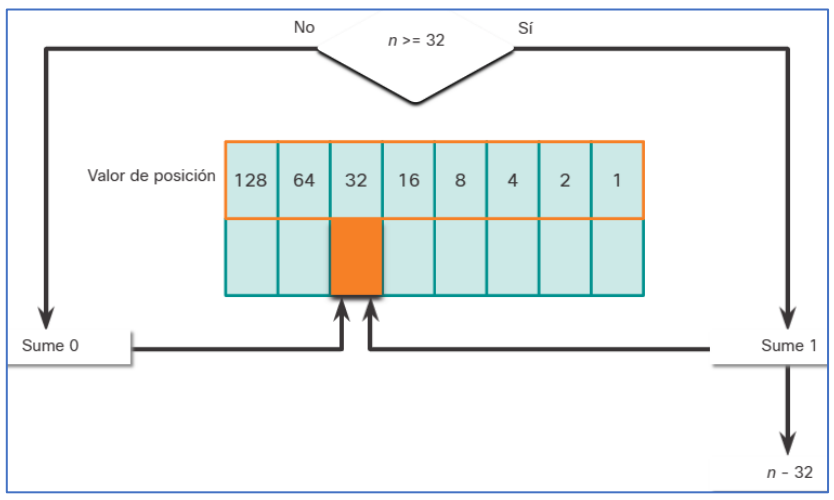
- Si no es así, introduzca un valor binario **0** en el valor de posición **64**.
- Si es así, agregue un valor binario **1** al valor de posición **64** y reste **64** del número decimal.



32

¿Es el número decimal del octeto (n) igual o mayor que el siguiente bit más significativo (**32**)?

- Si no es así, introduzca un valor binario **0** en el valor de posición **32**.
- Si es así, agregue un valor binario **1** al valor de posición **32** y reste **32** del número decimal.



Proceder similarmente para 16,8,4,2 y 1.

3.1.6 Ejemplo de Conversión de Decimal a Binario

Para poder comprender el proceso, considere la dirección IP 192.168.11.10. El primer octeto número 192 se convierte a binario utilizando el proceso de notación posicional explicado anteriormente.

Es posible omitir el proceso de resta con números decimales menores o más pequeños. Por ejemplo, observe que es bastante fácil calcular el tercer octeto convertido a un número binario sin pasar realmente por el proceso de resta (8 + 2 = 10). El valor binario del tercer octeto es 00001010.

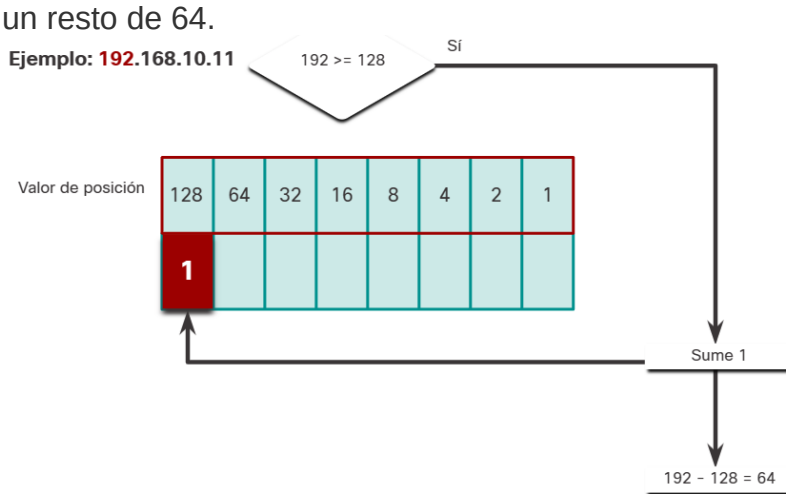
El cuarto octeto es 11 (8 + 2 + 1). El valor binario del cuarto octeto es 00001011.

La conversión de sistema binario a decimal puede parecer un desafío inicialmente, pero con la práctica resulta más fácil.

Haga clic en cada paso para ver la conversión de la dirección IP de 192.168.10.11 en binario.

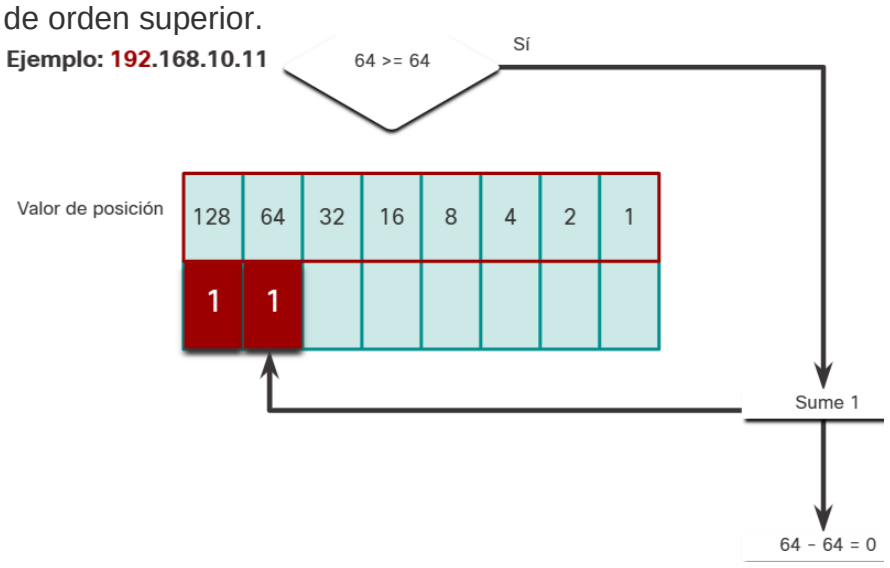
Paso 1

¿Es el primer octeto número 192 igual o mayor que el bit de orden superior 128? Sí lo es, por lo tanto, agregue un 1 al valor posicional de orden superior para representar 128. Resta 128 de 192 para producir un resto de 64.



Paso 2

¿Es el resto 64 igual o mayor que el siguiente bit de orden superior 64? Es igual, por lo tanto, agregue un 1 al siguiente valor posicional de orden superior.



Paso 3: Dado que no hay resto, introduzca el 0 binario en los valores posicionales restantes. El valor binario del primer octeto es 11000000.

Proceder similarmente con los demás octetos:

11000000 . 10101000 . 00001010 . **00001011**

3.1.7 Actividad - Conversión de Decimal a Binario

Esta actividad le permite practicar la conversión de valores decimales a valores binarios de 8 bits. Le recomendamos que trabaje con esta herramienta hasta que pueda realizar la conversión sin errores. Convierta el número decimal mostrado en la fila Valor decimal a sus bits binarios.

Valor decimal	68							
Base	2	2	2	2	2	2	2	2
Exponente	7	6	5	4	3	2	1	0
Posición	128	64	32	16	8	4	2	1
Bit	0	1	0	0	0	1	0	0

3.1.8 Actividad - Juego Binario

Esta es una forma divertida de aprender números binarios para redes.

Enlace del Juego: https://learningnetwork.cisco.com/docs/DOC-1803

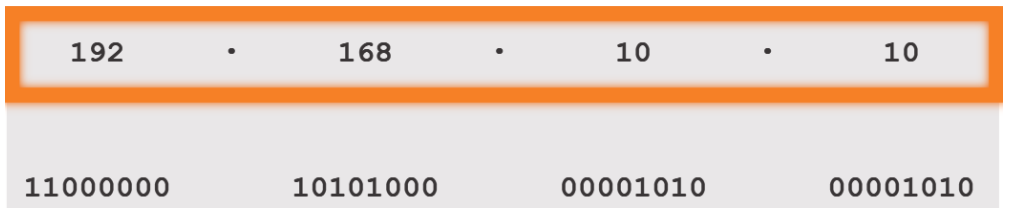
Deberá iniciar sesión en cisco.com para utilizar este enlace. Será necesario crear una cuenta si aún no tiene una.

También hay una variedad de juegos binarios móviles gratuitos. Busque "Juego Binario" en su tienda de aplicaciones.

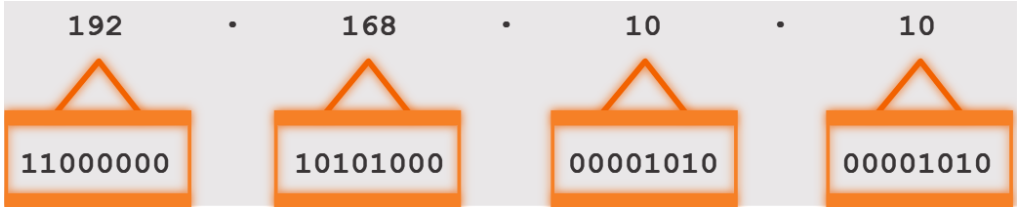
3.1.9 Direcciones IPv4

Como se mencionó al principio de este tema, los enrutadores y las computadoras solo entienden binario, mientras que los humanos trabajan en decimal. Es importante que usted conozca a fondo estos dos sistemas de numeración y cómo se utilizan en redes.

192.168.10.10 es una dirección IP asignada a una computadora.



La dirección se compone de cuatro octetos diferentes.



La computadora almacena la dirección como el flujo de datos total de 32 bits.

192	168	10	10
11000000	10101000	00001010	00001010

2. Sistema numérico hexadecimal

3.2.1 Direcciones Hexadecimales e IPv6

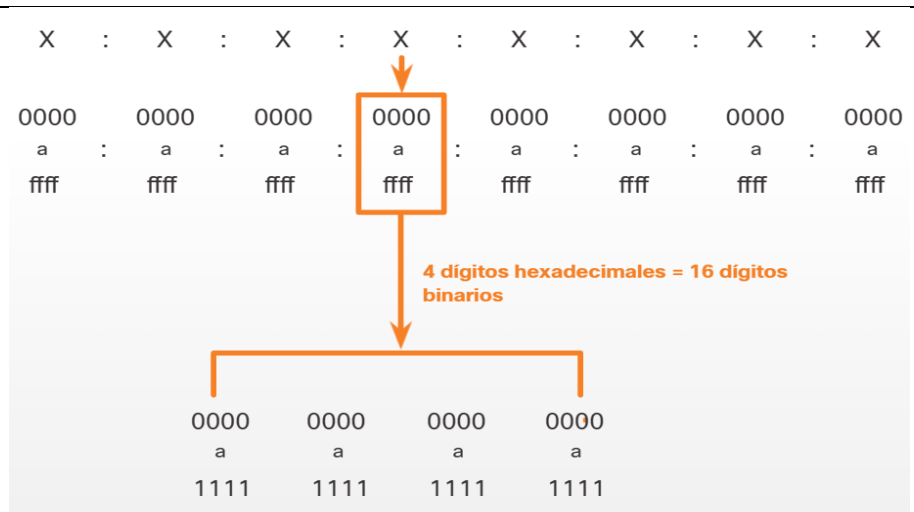
Ahora sabes cómo convertir binario a decimal y decimal a binario. Necesita esa habilidad para comprender el direccionamiento IPv4 en su red. Pero es igual de probable que use direcciones IPv6 en su red. Para entender las direcciones IPv6, debe ser capaz de convertir hexadecimal a decimal y viceversa.

Así como el decimal es un sistema de base diez, el hexadecimal es un sistema de base dieciséis. El sistema base de dieciséis números usa los dígitos del 0 al 9 y las letras de la A a la F. La figura muestra los valores decimales y hexadecimales equivalentes para el binario 0000 a 1111.

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

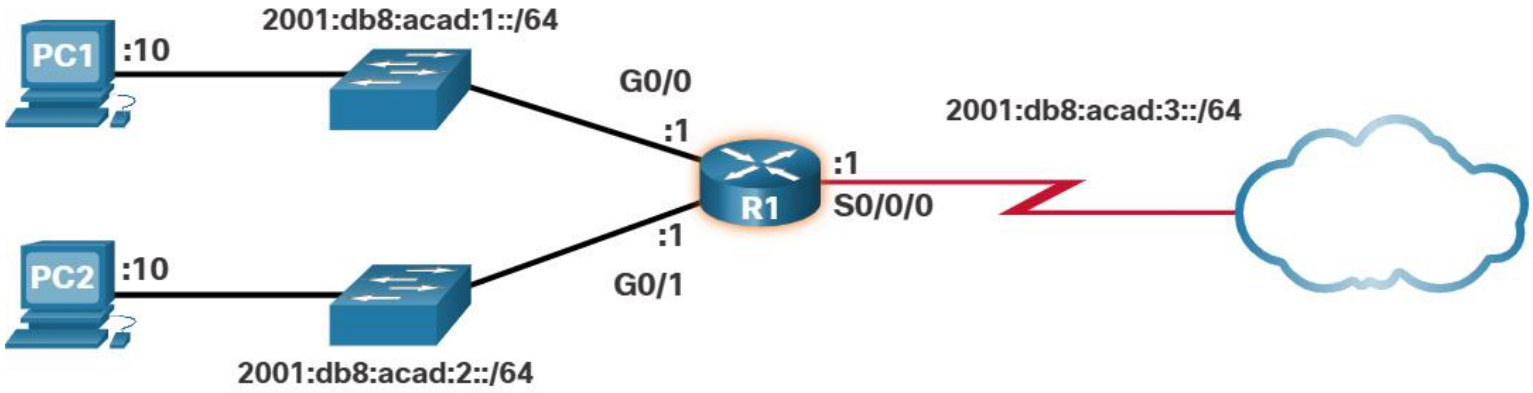
Binario y hexadecimal funcionan bien juntos porque es más fácil expresar un valor como un solo dígito hexadecimal que como cuatro bits binarios.

El sistema de numeración hexadecimal se usa en redes para representar direcciones IP Versión 6 y direcciones MAC Ethernet.



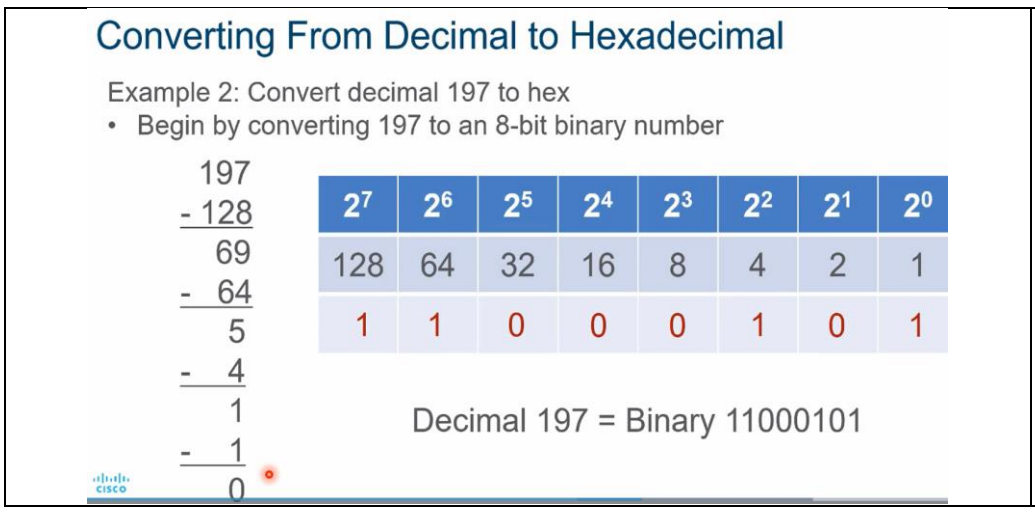
Las direcciones IPv6 tienen una longitud de 128 bits y cada 4 bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas.
Como se muestra en la figura, el formato preferido para escribir una dirección IPv6 es x: x: x: x: x: x: x: x, donde cada "x" consta de cuatro valores hexadecimales. Al hacer referencia a 8 bits de una dirección IPv4, utilizamos el término “octeto”. En IPv6, un hexteto es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada “x” es un único hexteto, 16 bits o cuatro dígitos hexadecimales.

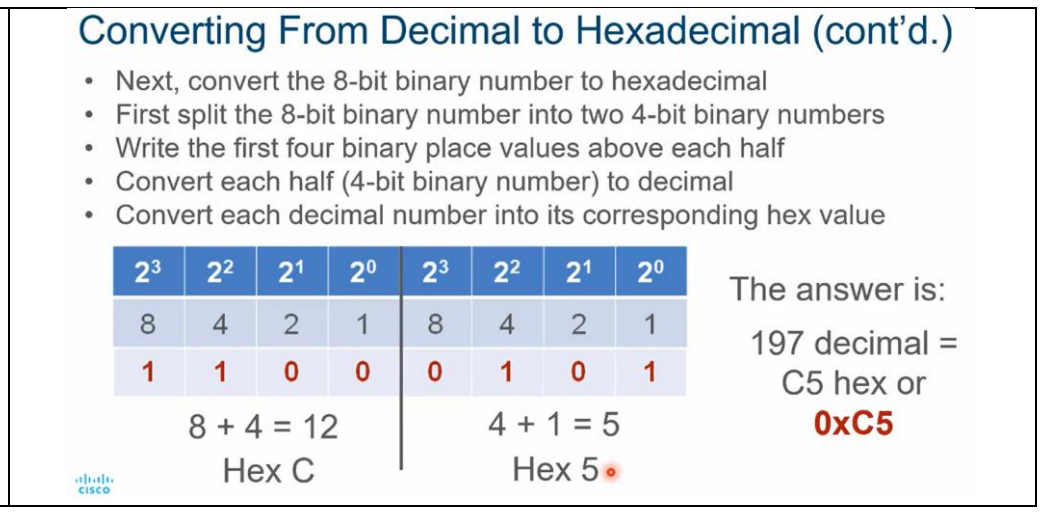
La topología de ejemplo de la figura muestra direcciones hexadecimales IPv6.



3.2.2 Vídeo - Conversión Entre Sistemas de Numeración Hexadecimal y Decimal

Hexadecimal o hex para abreviar, es un sistema numérico de base 16. Utiliza 16 símbolos, los números del cero al 9 así como las letras de la A a la F se basa en potencias de 16. Si seguimos el mismo procedimiento utilizado para convertir de binario a decimal, podemos escribir los valores de lugar o la notación posicional también para el sistema numérico hexadecimal. Aquí podemos ver los primeros cuatro valores posicionales basados en potencias de 16. Esto es 16 elevado a 0=1, cualquier número elevado a cero es uno. Esto es 16 elevado a 1 o 16. Esto es 16 elevado a potencia de dos o 16 * 16 que es igual a 256, y esto es 16 a la potencia de tres o 16 * 16 * 16 que es igual a 4096. Veamos la equivalencia decimal y binaria de cada símbolo hexadecimal. Estos son los equivalentes decimales. Tenga en cuenta que el símbolo hexadecimal A es igual al decimal 10. El hexadecimal B es igual al decimal 11 y así sucesivamente hasta llegar al hexadecimal F, que es igual al decimal 15. Aquí están los equivalentes binarios. Tenga en cuenta que cada símbolo hexadecimal se puede utilizar para representar un número binario de cuatro bits. Dado que ocho bits es una agrupación binaria común, podemos representar un número binario de 8 bits usando solo dos símbolos hexadecimales. En este primer ejemplo, veamos cómo convertir Hex 28 a decimal. Primero escribiré la notación posicional para las primeras 2 potencias de 16, luego insertaré los símbolos hexadecimales debajo de los valores posicionales correspondientes dos debajo de 16 y uno debajo de uno. Luego multiplicaré cada símbolo hexadecimal por el valor posicional bajo el cual se encuentra y sumamos los resultados. Entonces obtenemos (2*16)+(A*1)=(32)+(10*1)=42 en decimal. Multiplicar o dividir por 16 no siempre es fácil cuando se hace conversiones de hexadecimal a decimal. Primero convertiremos el decimal 197 a hexadecimal. Comenzaré convirtiendo 197 en un número binario de 8 bits. Aquí extraje los primeros ocho valores posicionales del sistema numérico binario. Necesitamos averiguar qué combinación de estos valores posicionales suma 197. Comenzaré escribiendo 197 en el lado izquierdo. Y comenzando por la izquierda, si el valor posicional es igual o menor que este número, Pongo A1 debajo y lo resto, y si es mayor, pongo un cero debajo y paso al siguiente valor posicional. Como puedo restar 128 de 197, pondré A1 debajo y lo restaré. Y eso me da 69. Puedo restar 64 de 69, así que pondré A1 debajo y lo restaré. Eso me da 532 es demasiado grande, así que pondré un cero debajo de eso. 16 también es demasiado grande, por lo que obtener un 08 también es demasiado grande. Pero cuando llego a 4 puedo restar eso. Así que pongo un uno ahí y lo resto. Aquí dos es demasiado, así que cero va allí y uno es justo. Así que lo resto y da como resultado un cero. Por lo tanto, el decimal 197 es igual a binario. 11000101. A continuación, convertiré el número binario de 8 bits en decimal dividiéndolo primero en dos números binarios de cuatro bits, y luego reescribiré los primeros cuatro valores posicionales binarios encima de cada mitad. Así que aquí tener 1248 y luego repetirlo a la izquierda 1248. Luego convertiré cada mitad a decimal y luego cada decimal a su valor hexadecimal equivalente. En el lado izquierdo tenemos 8 + 4 que es igual a 12, y en el lado derecho tenemos 4 + 1, que es igual a cinco si convertimos. Esos dos decimales hexadecimales 12 son el equivalente de C y hexadecimal, y cinco decimales son el equivalente de cinco en hexadecimal. Por lo tanto, 197 en decimal es C5 y hexadecimal, o también se puede escribir con un 0X precediéndolo para indicar que lo que sigue está escrito en hexadecimal. Por último, veamos la conversión de hexadecimal a decimal, pero esta vez primero convertiremos a binario en lugar de ir directamente a decimal como hice en el primer ejemplo, primero convertiré el hexadecimal 9F a decimal, convertiré cada símbolo hexadecimal a su equivalente binario de cuatro bits. Tengo HEX 9 que es el igual que decimal 9 y eso me da 1001. Y luego tengo hexadecimal F que es equivalente a decimal 15 y eso me da 1111 en binario. Luego los combinaré en un número binario de 8 bits. Así que aquí tengo los primeros ocho coloque los valores en binario y luego los convertiré a decimal y eso me da 128. Más 16 + 8 + 4 + 2 + 1 o 159 en decimal. A menudo hay varias formas de abordar la conversión entre sistemas numéricos. Debes usar el que mejor te funcione.





3.2.3 Verifique su Comprensión - Convierta entre Sistemas Numéricos Decimales a Hexadecimales

¿Cuál es el equivalente hexadecimal de 202?	¿Cuál es el equivalente hexadecimal de 254?	¿Cuál es el equivalente decimal de A9?	¿Cuál de los siguientes es el equivalente decimal de 7D?
B10	EA	168	124
BA	ED	✓ 169	✓ 125
C10	FA	170	126
✓ CA	✓ FE	171	127

3. Resumen de sistemas numéricos

3.3.1 ¿Qué Aprendí en este Módulo?

Sistema de numeración binario

Binario es un sistema de numeración que consta de los dígitos 0 y 1 llamados bits. En contraste, el sistema de numeración decimal consta de 10 dígitos que consisten en los dígitos desde el 0 al 9. Los hosts, los servidores y los dispositivos de red utilizan direccionamiento binario. Específicamente, utilizan direcciones IPv4 binarias. Para facilitar el uso por parte de las personas, las direcciones IPv4 se expresan comúnmente en notación decimal punteada.

Este sistema decimal utiliza las potencias de diez, o base 10. Por ejemplo, el número 2,146 tiene un 2 en el lugar de miles, o dos mil. 2,146 tiene un 1 en el lugar de las cientos, o cien. Tiene un 4 en el lugar de las decenas, o cuarenta. Tiene un 6 en el lugar de las unidades, o seis.

El sistema binario es un sistema numérico de base 2. Cada valor posicional puede tener un 0 o un 1. La tabla de valores de posición binarios es una herramienta útil. Es común utilizar una tabla con ocho marcadores de posición. 8 bits equivalen a un byte.

Sistema numérico hexadecimal

El sistema de numeración hexadecimal se usa en redes para representar direcciones IP Versión 6 y direcciones MAC Ethernet. Este sistema numérico de base dieciséis utiliza los dígitos del 0 al 9 y las letras de la A a la F. El binario y el hexadecimal funcionan bien juntos porque es más fácil expresar un valor como un solo dígito hexadecimal que como cuatro bits binarios.

Las direcciones IPv6 tienen una longitud de 128 bits y cada 4 bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas.

3.3.2 Webster - Preguntas de Reflexión

No esperaba hacer matemáticas en medio de mi curso de redes, pero me sorprendió lo divertido que es convertir números decimales en sus equivalentes binarios y hexadecimales. Tengo una mejor comprensión de por qué las direcciones IP se representan de la manera en que las vemos. Antes de tomar este módulo, ¿qué sabía sobre los sistemas de numeración binarios y hexadecimales? Eche un vistazo a la dirección MAC en la NIC de su computadora. ¿Qué reconoces acerca de esta dirección que quizás no hayas notado antes?

3.3.3 Prueba de Sistemas Numéricos

¿Cuál es la representación binaria del número decimal 173? 10100111 10100101 ✓ 10101101 10110101	¿Cuántos bits componen un octeto en una dirección IPv4? 4 ✓ 8 16 32	¿Cuál es el equivalente decimal de 0xC9? 185 200 ✓ 201 199	¿Cuál es la representación de 0xCA en sistema binario? 10111010 11010101 ✓ 11001010 11011010
¿Cuál es el rango de valores hexadecimales que se pueden utilizar en un hexteto? De 0000 a 1111 ✓ De 0000 a ffff De 1111 hasta aaaa De 0000 a 9999	¿Cuál es el equivalente hexadecimal del número binario 10011101? 85 ✓ 9D A1 D9	¿Cuántos bits hay en una dirección IPv4? ✓ 32 64 128 256	¿Cuál es el equivalente hexadecimal del número decimal 139? ✓ 8B 92 A1 D7
Un ingeniero de redes desea representar datos confidenciales en formato binario. ¿Cuáles son los dos valores posibles que puede utilizar el ingeniero? (Elija dos opciones). ✓ 0 ✓ 1 2 A F	¿Cuál es un número hexadecimal válido? ✓ f g h j	¿Cuál es el equivalente binario del número decimal 232? ✓ 11101000 11000110 10011000 11110010	Dada la dirección binaria de 11101100 00010001 00001100 00001010, ¿qué dirección representa esto en formato decimal de puntos? 234.17.10.9 234.16.12.10 236.17.12.6 ✓ 236.17.12.10

Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 1 – 3

Bienvenido al Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 1 - 3.

Esta evaluación cubre los conceptos básicos y las habilidades presentadas en los Módulos 1 a 3 del curso Dispositivos de Red y Configuración Inicial. Hay 21 preguntas en total. Debe alcanzar el 70% para aprobar este examen. Tiene intentos ilimitados para aprobar el examen. Se proporcionan comentarios para dirigirlo a áreas que pueden requerir atención adicional.

El contenido de Cisco Networking Academy está protegido por leyes de derechos de autor y está prohibido publicar, distribuir o compartir el contenido de este examen sin autorización.

© 2022, Cisco Systems, Inc.

¿Cuál función depende de la priorización del tráfico de red y se utiliza para garantizar la prestación exitosa de servicios en tiempo real?

Redundancia	Calidad de servicio ←☺	Confiabilidad	Seguridad

Un administrador agrega capacidades de servicio de voz y video a una red existente. ¿Qué requisito de diseño satisface esta situación?

Seguridad	Facilidad de administración	Escalabilidad ←☺	Disponibilidad

¿Qué tipo de dirección se asigna físicamente a la NIC de una estación de trabajo?

Dirección de host	Dirección de red	Dirección IP	Dirección MAC ←☺

¿Cuál es una característica de un hipervisor de tipo 2?

No requiere software de consola de administración ←☺	Mas adecuados para entornos empresariales
Se instalan directamente en el hardware	Tienen acceso directo a recursos de hardware de servidores

Explicación: Los hipervisores de tipo 2 se alojan en un sistema operativo subyacente, y se adaptan mejor a las aplicaciones de clientes finales y de experimentación con la virtualización. A diferencia de los hipervisores de tipo 1, los hipervisores de tipo 2 no requieren de una consola de administración y no tienen acceso directo al hardware.

Una universidad construye una nueva residencia estudiantil en su campus. Los trabajadores cavan para instalar las nuevas tuberías de agua de la residencia. Uno de ellos accidentalmente daña el cable de fibra óptica que conecta dos de las residencias existentes al centro de datos del campus. A pesar de que se cortó el cable, los estudiantes de las residencias solo perciben una interrupción muy breve en los servicios de red. ¿Qué característica de la red se demuestra aquí?

QoS ←☺	Tolerancia a fallas	Integridad	Escalabilidad	Seguridad

Haga coincidir la capa de diseño jerárquico con la descripción.

Capa de distribución	✓ Proporciona conexión de alta velocidad para la red troncal
Capa de núcleo	✓ Proporciona conectividad a los hosts de la red
Capa de acceso	✓ Proporciona interconexiones para redes de acceso local más pequeñas

¿Qué característica define una nube privada?

Para una comunidad especifica	Para el público en general	Para una organización especifica ←☺	Compuesto por dos o más nubes

¿Cuál capa del modelo de diseño jerárquico proporciona un medio para conectar dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red?

Núcleo	Aplicación	Distribución	Red	Acceso ←☺

¿Qué servicio de computación en la nube es el más adecuado para una organización que necesita crear aplicaciones en colaboración y enviarlas por la web?

IaaS	ITaaS	SaaS	PaaS ←☺

¿Cuál es el equivalente decimal del número binario 10111010?

D9	BA ←☺	A1	85

¿Cuántos valores únicos son posibles con un solo dígito binario?

2 ←☺	4	8	1

Un técnico de redes está trabajando en la red inalámbrica en una clínica médica. El técnico configura accidentalmente la red inalámbrica para que los pacientes puedan ver los datos de los registros médicos de otros pacientes. ¿Cuál de las cuatro características de la red se ha violado en esta situación?

Confiabilidad	Escalabilidad	Seguridad ←☺	Tolerancia a fallas	Calidad de servicio

¿Qué formato de dirección IPv4 se creó para facilitar el uso de las personas y se expresa como 201.192.1.14?

Binario	ASCII	Decimal punteada ←☺	Hexadecimal

¿Cuál es el equivalente decimal del valor hexadecimal 3F?

45	46	63 ←☺	18	34

Un estudiante está aprendiendo sistemas numéricos. ¿Cuál es el equivalente hexadecimal del número decimal 165?

A5 ←☺	9F	7D	C8

¿Cuál es la función principal de un hipervisor?

Crear máquinas virtuales (VMs) y proporcionar abstracción de hardware para admitirlas ←☺
Crear un entorno aislado donde se ejecutan aplicaciones en contenedores

Realizar funciones de FCAPS para VNF
Centralizar la administración de la configuración de Switch

Explicación: Un hipervisor es un proceso de software que abstrae la capa de hardware de los sistemas operativos y permite que varias máquinas virtuales se ejecuten simultáneamente.

Una empresa utiliza un sistema de nómina basado en la nube. ¿Qué tecnología de computación en la nube utiliza esta empresa?

Software como Servicio (SaaS) ←☺	Conexión inalámbrica como Servicio (WaaS)
Plataforma como Servicio (PaaS)	Infraestructura como Servicio (IaaS)

¿Qué enunciado describe con precisión un hipervisor de tipo 2?

Es el tipo más común de hipervisor en los centros de datos empresariales
Se encuentra directamente sobre el hardware y proporciona la capacidad de virtualizar el hardware para varias máquinas virtuales
Es comúnmente un sistema operativo de código abierto
Se ejecuta como una capa de software sobre un sistema operativo host ←☺

¿Cuál es la representación decimal punteada de la dirección IPv4 que se representa como la cadena binaria: 00001010.01100100.00010101.00000001?

10.10.20.1	100.10.11.1	100.21.10.1	10.100.21.1 ←☺

Una empresa está considerando implementar soluciones de virtualización en un centro de datos. ¿Cuáles son las tres ventajas de la virtualización de las que la empresa puede esperar beneficiarse? (Elija tres).

Aprovisionamiento más rápido de servidores ←☺	Mejor recuperación tras un desastre ←☺
Semana laboral más corta	Requisitos de espacio físico reducido ←☺
Reducción de los requisitos de seguridad	Menos capacitación de empleados

¿Cuáles son las dos diferencias entre los números binarios y los decimales? (Elija dos opciones).

- ✓ Los números binarios se basan en las potencias de 2.
- Los números que se escriben en un teclado se ingresan como binarios y la computadora los convierte en decimales.
- Los números decimales se basan en las potencias de 1.
- Los números binarios constan de tres estados: activado, desactivado, nulo. Los números decimales no tienen estados.
- ✓ Los números decimales incluyen 0 a 9.

Módulo 4: Conmutación Ethernet

0. Introducción

4.0.1 Webster - ¿Por Qué Debería Tomar este Módulo?

¡Hola! ¡Es Webster otra vez! Marcy y Vincent comienzan a ver el valor de los consejos de Bob. Pero no pueden permitirse mucho tiempo de inactividad y deben operar con la red existente hasta que Bob pueda realizar las actualizaciones. Hasta entonces, no agregarán VoIP, cámaras de seguridad ni el sistema de pedidos en línea. Bob debe evaluar su red existente antes de la actualización para comprender mejor lo que se debe hacer.

La red de la mueblería es una red Ethernet. Los protocolos de Ethernet definen cómo se formatean los datos y cómo se transmiten a través de la red cableada y especifican los protocolos que operan en la Capa 1 y la Capa 2 del modelo OSI.

¿Está familiarizado con Ethernet? ¿Por qué son importantes los sistemas numéricos hexadecimales y binarios en una red Ethernet? ¡Creo que debería aprovechar este módulo para obtener más información sobre Ethernet, tramas Ethernet y direcciones MAC Ethernet! Comencemos ya mismo.

4.0.2 ¿Qué Aprenderé en este Módulo?

Título del Módulo: Conmutación Ethernet

Objetivo del Módulo: Explicar cómo funciona Ethernet en una red conmutada.

Título del Tema	Objetivo del Tema
Ethernet	Explique las funciones de capa 1 y capa 2 del modelo OSI en una red Ethernet.
Tramas de Ethernet	Explique la forma en que las subcapas de Ethernet se relacionan con los campos de trama.
Dirección MAC de Ethernet	Explicar los tipos de direcciones MAC Ethernet.
La Tabla de Direcciones MAC	Explique la forma en que un switch arma su tabla de direcciones MAC y reenvía las tramas.

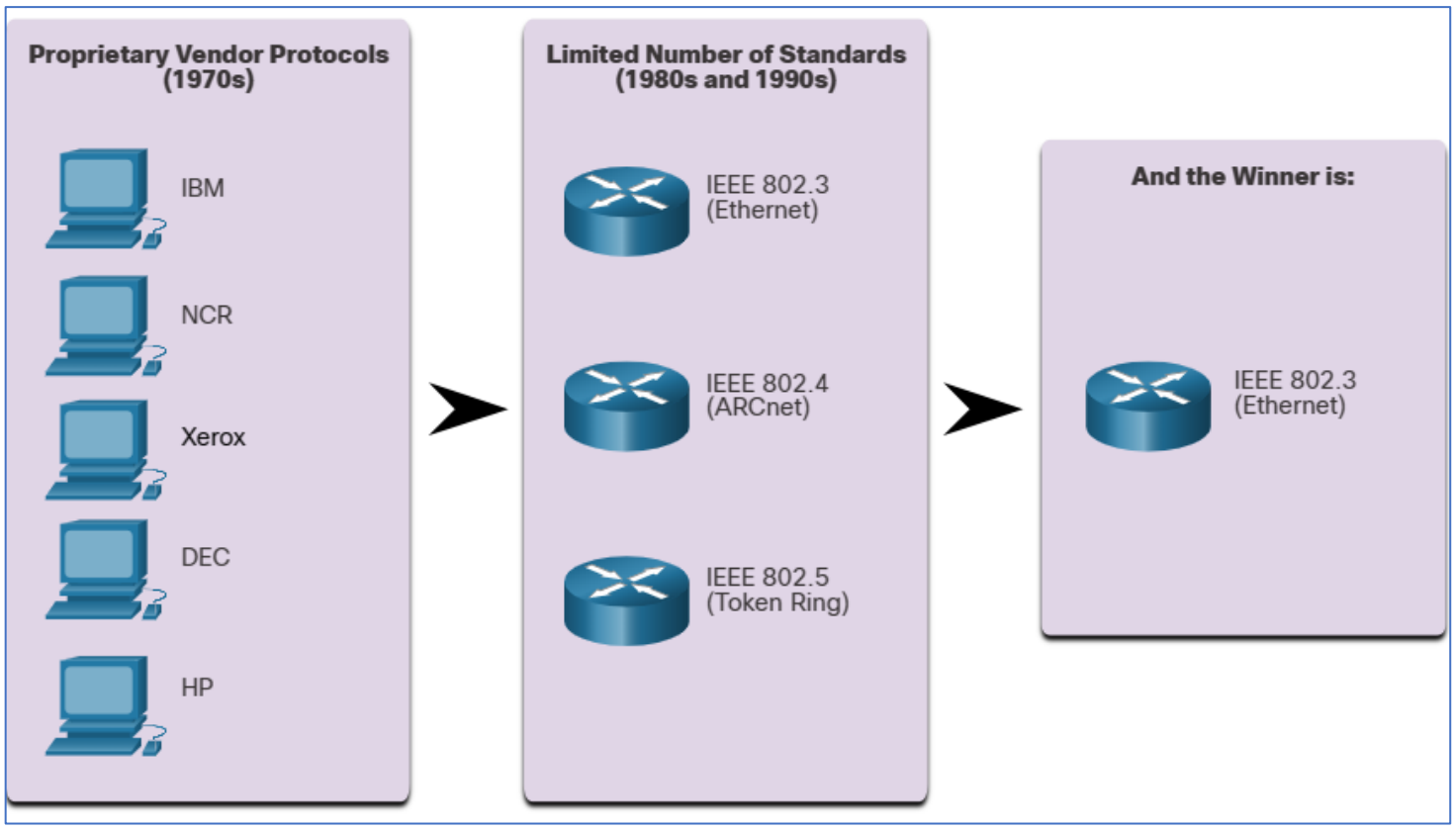
1. Ethernet

4.1.1 El Auge de Ethernet

En los comienzos de las redes, cada fabricante utilizaba sus propios métodos para la interconexión de los dispositivos de red y los protocolos de red. Si compró equipos de otros proveedores, nadie podía garantizarle que funcionen bien juntos. Los equipos de un proveedor podrían no comunicarse con los de otro fabricante. A medida que se generalizó el uso de las redes, se desarrollaron estándares que definían las reglas con las que operaban los equipos de red de los diferentes fabricantes. Los estándares resultan beneficiosos para las redes de muchas maneras:

- Facilitan el diseño
- Simplifican el desarrollo de productos
- Promueven la competencia
- Proporcionan interconexiones coherentes
- Facilitan la capacitación
- Proporcionan más opciones de fabricantes a los clientes

No hay un protocolo oficial estándar para las redes locales, pero con el tiempo la tecnología Ethernet se volvió más habitual que las demás. Los protocolos de Ethernet definen qué formato tienen los datos y cómo se transmiten por la red cableada. Los estándares de Ethernet especifican protocolos que funcionan en la capa 1 y en la capa 2 del modelo OSI. Se ha convertido en un estándar de facto, lo que significa que Ethernet es la tecnología que se utiliza en casi todas las redes de área local cableadas, tal como se indica en la figura.



4.1.2 Evolución de Ethernet

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) lleva un control de los estándares de redes, incluidos los estándares Ethernet e inalámbricos. Los comités del IEEE son responsables de aprobar y mantener los estándares para conexiones, requisitos de medios y protocolos de comunicación. A cada estándar de tecnología se le asigna un número que hace referencia al comité que es responsable de aprobar y mantener el estándar. El comité responsable de los estándares de Ethernet es el 802.3.

Desde la creación de Ethernet en 1973, los estándares evolucionaron para especificar versiones más rápidas y flexibles de la tecnología. Esta capacidad que tiene Ethernet de evolucionar con el paso del tiempo es una de las principales razones por las que se ha popularizado. Cada versión de Ethernet tiene un estándar asociado. Por ejemplo: 802.3 100BASE-T representa los estándares de Ethernet de 100 Megabits utilizando cables de par trenzado. La notación del estándar se traduce de la siguiente manera:

- 100 es la velocidad en Mbps
- BASE significa transmisión en banda base.
- T es el tipo de cable, en este caso, par trenzado (Twisted).

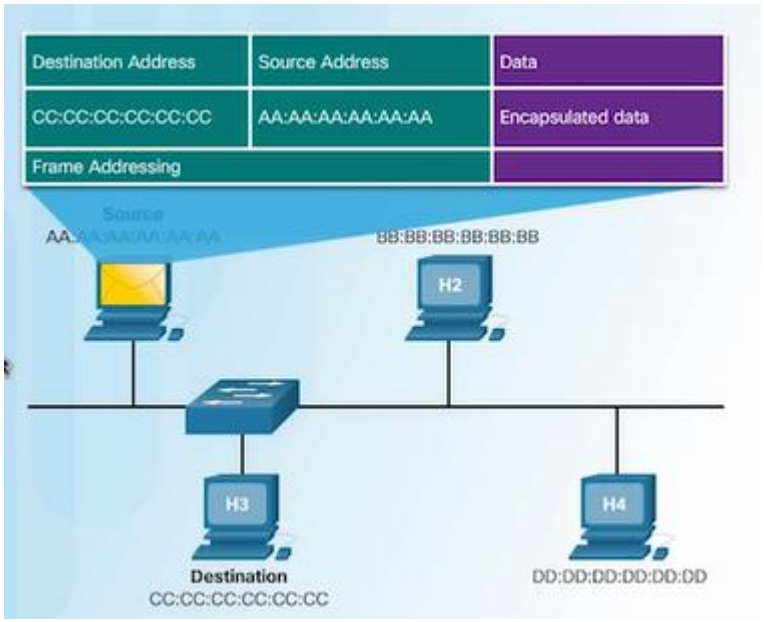
Las primeras versiones de Ethernet eran relativamente lentas, con una velocidad de 10 Mbps, Las versiones más recientes de Ethernet funcionan a 10 Gb/s e, incluso, más rápido. Imagine cuánto más rápidas son estas nuevas versiones que las redes Ethernet originales.

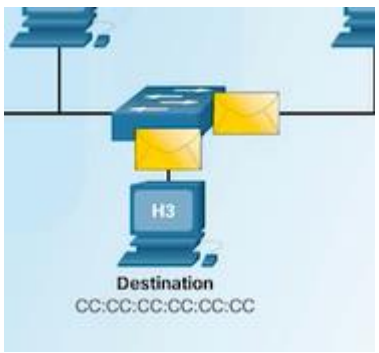
Year	2009	2015	2016 to present
Standard	802.3at (PoE)	100GbE and 40GbE	2.5GBASE-T and 5GBASE-T
Description	Power over Ethernet enhancements	100G/40G for optical fiber	2.5 Gigabit and 5 Gigabit Ethernet over twisted pair

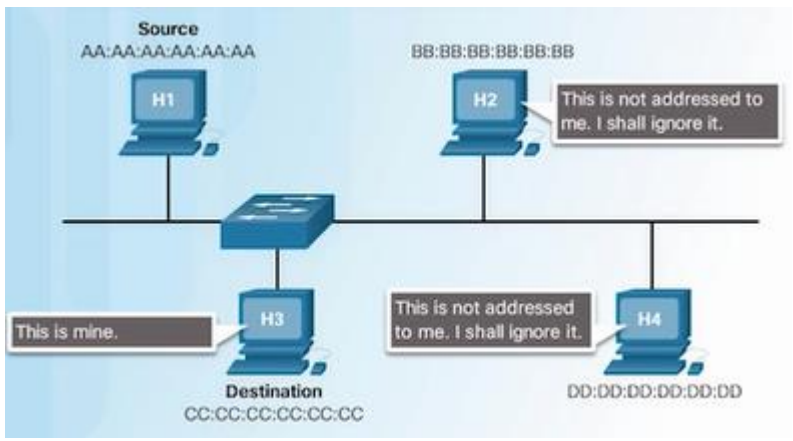
4.1.3 Vídeo - Direccionamiento Ethernet

En este video, vamos a ver un video de direccionamiento de Ethernet. Entonces, en nuestra topología, como puede ver, tenemos hosts H1H2H3 y H4. Mac significa control de acceso a medios. H1 tiene la dirección Mac de origen todas As. Entonces, avancemos y comencemos la animación y podemos ver que el host H1 tiene un frame o marco Ethernet para enviar al host H3. Entonces, en el marco Ethernet, hay una dirección Mac de destino que corresponde a la del host H3 que como puede ver es todo Cs. La dirección Mac de origen es la del host H1 todas As. Entonces, H1 envía esa trama de Ethernet al conmutador. Cuando el conmutador recibe esta trama de Ethernet, en este caso, va a reenviar la trama de Ethernet por todos sus puertos excepto el puerto de entrada. Más adelante, aprenderemos más acerca de cómo los conmutadores Ethernet pueden realmente filtrar los marcos, de modo que solo envíen el marco a su destino. Como puede ver, todos los dispositivos en la red reciben la trama

Ethernet, en este caso H2 y H4 también, pero estos dos hosts ignoran la trama de Ethernet. ¿Por qué hacen eso? Examinaron la dirección Mac de destino, la compararon con su propia dirección Mac y como no hay coincidencia, ignoran el frame. En realidad, la tarjeta Ethernet Nic de cada host hace ese trabajo, al no haber match simplemente no recibe el mensaje. Cuando H3 recibe la trama Ethernet, compara la dirección Mac de destino en la trama Ethernet con su propia dirección Mac en su tarjeta Nic, al existir coincidencia, continúa y recibe el resto del marco y el mensaje es procesado.







4.1.4 Laboratorio - Determinar la Dirección MAC de un Host

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Determinar la dirección MAC de una computadora con Windows conectada a una red Ethernet a través del comando **ipconfig /all**.
- Analizar una dirección MAC para determinar cuál es el fabricante.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
PC	VLAN 1	192.168.1.2	255.255.255.0

Objetivos

- Determinar la dirección MAC de una computadora con Windows conectada a una red Ethernet a través del comando **ipconfig /all**.
- Analizar una dirección MAC para determinar cuál es el fabricante.

Aspectos básicos/situación

Cada computadora de una red Ethernet local tiene una dirección de control de acceso a medios (MAC) que está grabada en su Tarjeta de Interfaz de Red (NIC=Network Interface Card). Las direcciones MAC de las computadoras generalmente se muestran como 6 grupos de dos números hexadecimales separados por guiones o dos puntos (ejemplo: 15-EF-A3-45-9B-57). El comando **ipconfig /all** muestra la dirección MAC de la computadora. Podrá trabajar de forma individual o en equipo.

Recursos necesarios

- PC con Windows 10 y una tarjeta de interfaz de red (NIC) Ethernet como mínimo
- Conectividad a Internet

Instrucciones

Parte 1: Cómo localizar una dirección MAC en una computadora

En esta parte del laboratorio determinará la dirección MAC de una computadora con el comando **ipconfig** de Windows.

Paso 1: Mostrar información para el comando ipconfig /all

a. Haga clic con el botón secundario del mouse en el botón **Start** (Inicio) y seleccione **Command Prompt** (Línea de comandos).
b. Introduzca el comando **ipconfig /all** en la línea de comandos.

Paso 2: Ubique una dirección MAC (física) en el resultado obtenido mediante el comando *ipconfig /all*

Utilice la siguiente tabla ejemplo para completar la descripción del adaptador Ethernet y la dirección física (MAC):

Descripción	Dirección física
Respuesta de ejemplo: **Intel(R) Ethernet Connection I219-LM**	**Respuesta de ejemplo:** **54-EE-75-C3-2B-33**

La PC puede tener una o más tarjetas NIC con sus correspondientes direcciones MAC.

Parte 2: Cómo analizar las partes de una dirección MAC

Se asigna una dirección física a cada interfaz de red Ethernet en el momento de su creación. Estas direcciones tienen 48 bits (6 bytes) de largo y están expresadas en notación hexadecimal. Las direcciones MAC están compuestas de dos partes. Una parte de la dirección MAC, los primeros 3 bytes, representa el proveedor que fabricó la interfaz de red. Esta parte de la dirección MAC se llama **OUI (Identificador Único Organizacional).** Cada proveedor que desea producir y vender interfaces de red Ethernet debe registrarse ante el IEEE para obtener un OUI.

La segunda parte de la dirección, los 3 bytes restantes, son la ID única de la interfaz. Todas las direcciones MAC que comienzan con el mismo OUI deben tener valores únicos en los últimos 3 bytes.
En este ejemplo, la dirección MAC física para la interfaz LAN Ethernet es D4-BE-D9-13-63-00.

OUI del fabricante	Identificador único para la interfaz	Nombre del proveedor
D4-BE-D9	13-63-00	Dell Incorporated

Paso 2: Busque los proveedores que son los dueños registrados del OUI que incluyó en la tabla.

a. Wireshark.org ofrece una herramienta de búsqueda fácil de usar en https://www.wireshark.org/tools/oui-lookup.html. Use esta herramienta u otras en Internet para buscar otras maneras de identificar un OUI.
b. Use la información que encontró para actualizar la columna del proveedor en el cuadro del paso 1.

Intente conectar y desconectar los cables de red y los adaptadores de red, y emitir el comando ipconfig /all nuevamente. ¿Qué cambios puede ver? ¿Sigue apareciendo la dirección MAC? ¿Cambiará la dirección MAC?
Rpta: Si bien las direcciones IP pueden cambiar, las direcciones MAC permanecen iguales.

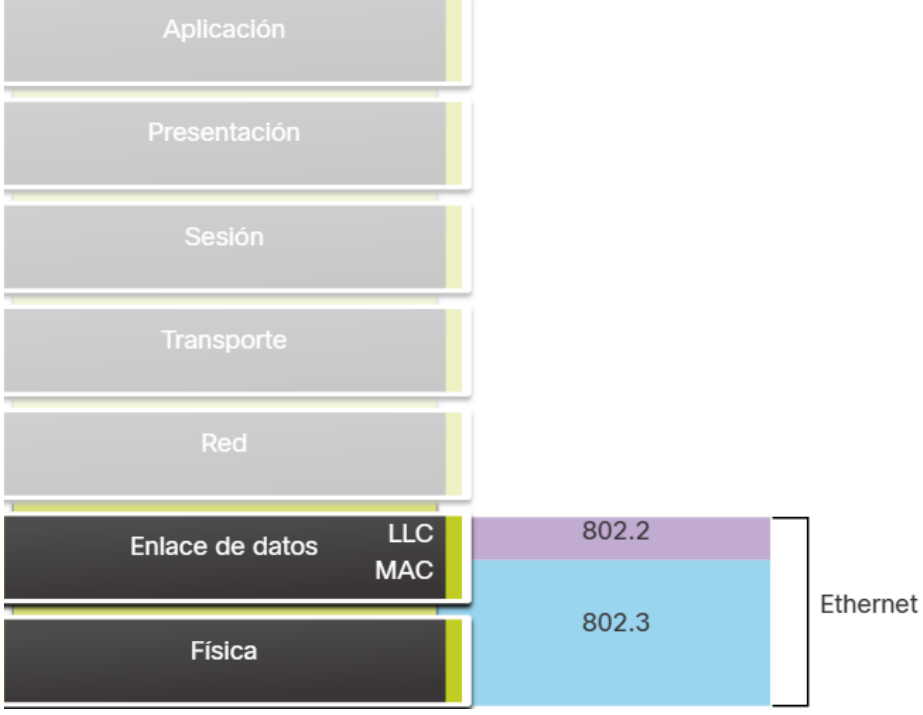
2. tramas de Ethernet

4.2.1 Encapsulación de Ethernet

Este módulo comienza con una discusión de la tecnología Ethernet incluyendo una explicación de la subcapa MAC y los campos de trama Ethernet. Ethernet es una de las dos tecnologías LAN utilizadas hoy en día, siendo la otra LAN inalámbricas (WLAN). Ethernet utiliza comunicaciones por cable, incluyendo pares trenzados, enlaces de fibra óptica y cables coaxiales.
Ethernet funciona en la capa de enlace de datos y en la capa física. Es una familia de tecnologías de redes definidas en los estándares IEEE 802.2 y 802.3. Ethernet soporta los siguientes anchos de banda de datos:

- 10 Mbps
- 100 Mbps
- 1000 Mbps (1 Gbps)
- 10.000 Mbps (10 Gbps)
- 40,000 Mbps (40 Gbps)
- 100,000 Mbps (100 Gbps)

Como se muestra en la figura, los estándares de Ethernet definen tanto los protocolos de Capa 2 como las tecnologías de Capa 1.
Ethernet y el modelo OSI

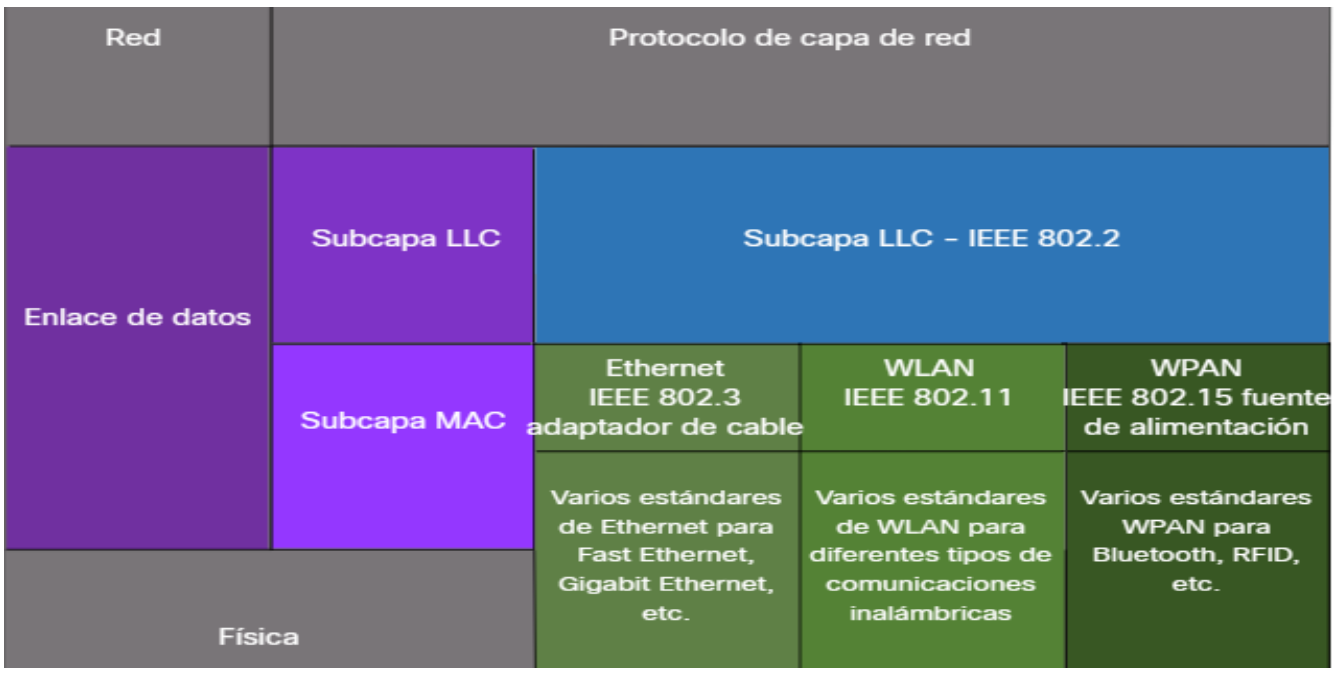


Ethernet se define mediante protocolos en la capa Física y en la capa Enlace de Datos.

4.2.2 Subcapas de la capa Enlace de Datos

Los protocolos IEEE 802 LAN/MAN, incluyendo Ethernet, operan en dos subcapas independientes en la capa Enlace de Datos: **Control de Enlace Lógico (LLC=Logical Link Control)** y **Control de Acceso a Medios (MAC)**, como se muestra en la figura. LLC y MAC tienen los siguientes roles en la capa de enlace de datos:

- **Subcapa LLC** - Esta subcapa IEEE 802.2 controla la interfaz de red haciendo uso de controladores de software, o sea comunica el software de red de Capa 3 con el hardware del dispositivo en Capa 1. Coloca en la trama, información que identifica qué protocolo de capa de Red se utiliza, como IPv4 e IPv6, permitiendo que ambos utilicen la misma interfaz de red y medios.
- **Subcapa MAC**- Esta subcapa (IEEE 802.3, 802.11 o 802.15, por ejemplo) se implementa en hardware y es responsable de la encapsulación de datos y el control de acceso a medios. Proporciona el direccionamiento de la capa Enlace de Datos y está integrada con varias tecnologías de capa física.



4.2.3 La Subcapa MAC

La subcapa MAC es responsable de la encapsulación de datos y del control de acceso a los medios.

Encapsulación de Datos

La encapsulación de datos IEEE 802.3 incluye lo siguiente:

- **Trama de Ethernet** - Esta es la estructura interna de la trama Ethernet.
- **Direccionamiento Ethernet** - La trama Ethernet incluye una dirección MAC de origen y destino para entregar la trama Ethernet, de NIC Ethernet a NIC Ethernet en la misma LAN.
- **Detección de Errores Ethernet** - La trama Ethernet incluye un tráiler de secuencia de verificación de trama (FCS=Frame Check Sequence) utilizado para la detección de errores.

Acceso a los Medios

Como se muestra en la figura, la subcapa MAC IEEE 802.3 incluye las especificaciones para diferentes estándares de comunicaciones Ethernet sobre varios tipos de medios, incluyendo cobre y fibra.

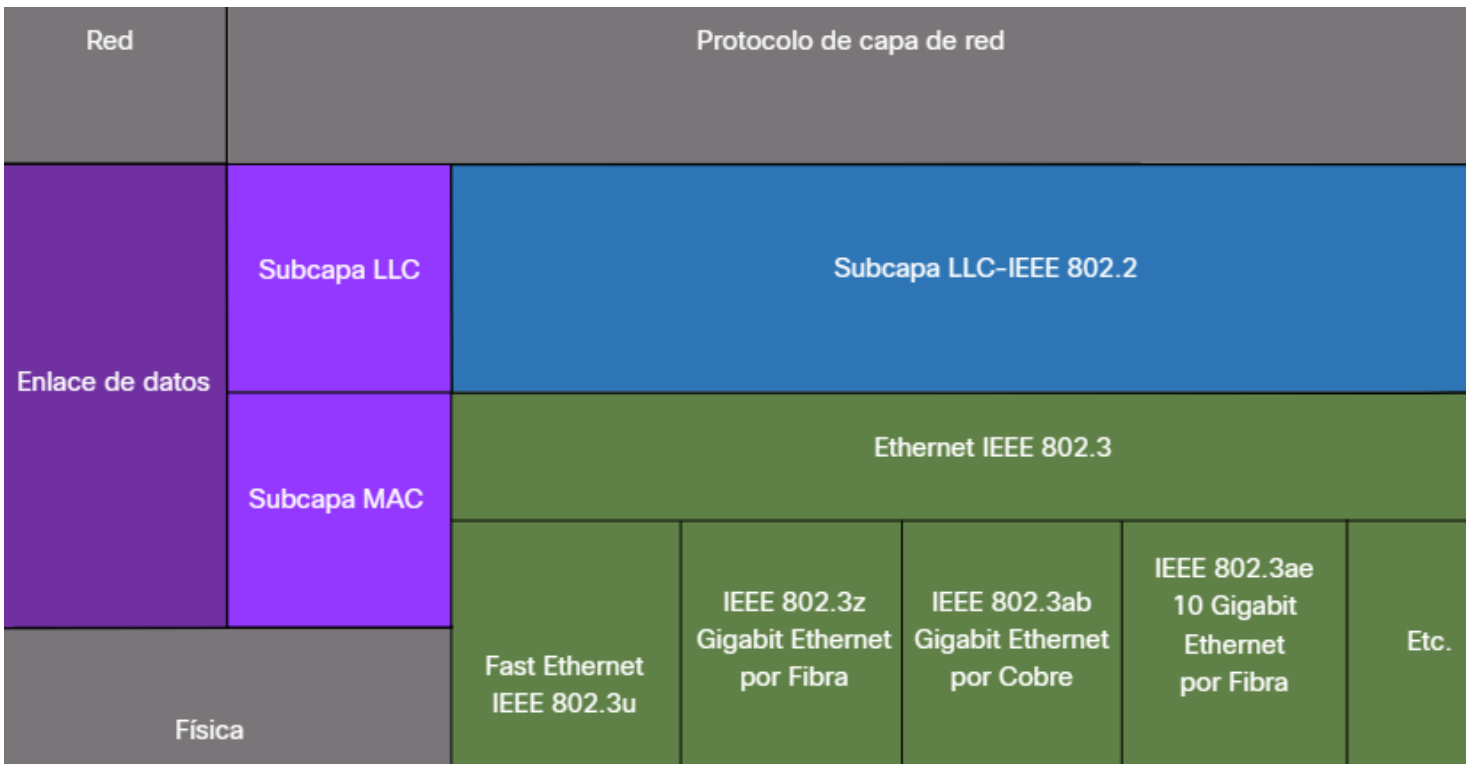


Fig. Estándares Ethernet en la Subcapa MAC

Recuerde que Ethernet heredado utilizaba una topología de bus o hubs, era *half-dúplex*. En esta topología el protocolo CSMA/CD garantizaba que sólo un dispositivo esté transmitiendo a la vez. CSMA/CD permitía que varios dispositivos compartan el mismo medio detectando una colisión cuando más de un dispositivo intentaba transmitir simultáneamente. También proporcionaba un algoritmo de retroceso para la retransmisión.

CSMA/CD son siglas que corresponden a **Carrier Sense Multiple Access with Collision Detection**, que corresponden a **Acceso Múltiple por Detección de Portadora con Detección de Colisiones**, era una técnica usada en las redes para mejorar las prestaciones.

Las LAN Ethernet de hoy utilizan switches que funcionan en *full-dúplex*. Las comunicaciones full-dúplex con switches Ethernet no requieren control de acceso a través de CSMA/CD.

4.2.4 Campos de la Trama de Ethernet

El tamaño mínimo de la trama de Ethernet es de 64 bytes y el máximo esperado es de 1518 bytes. Esto incluye todos los bytes desde el campo Dirección MAC Destino hasta el campo **Secuencia de Verificación de Trama (FCS=Frame Check Sequence)**. El campo preámbulo no se incluye al describir el tamaño de una trama.

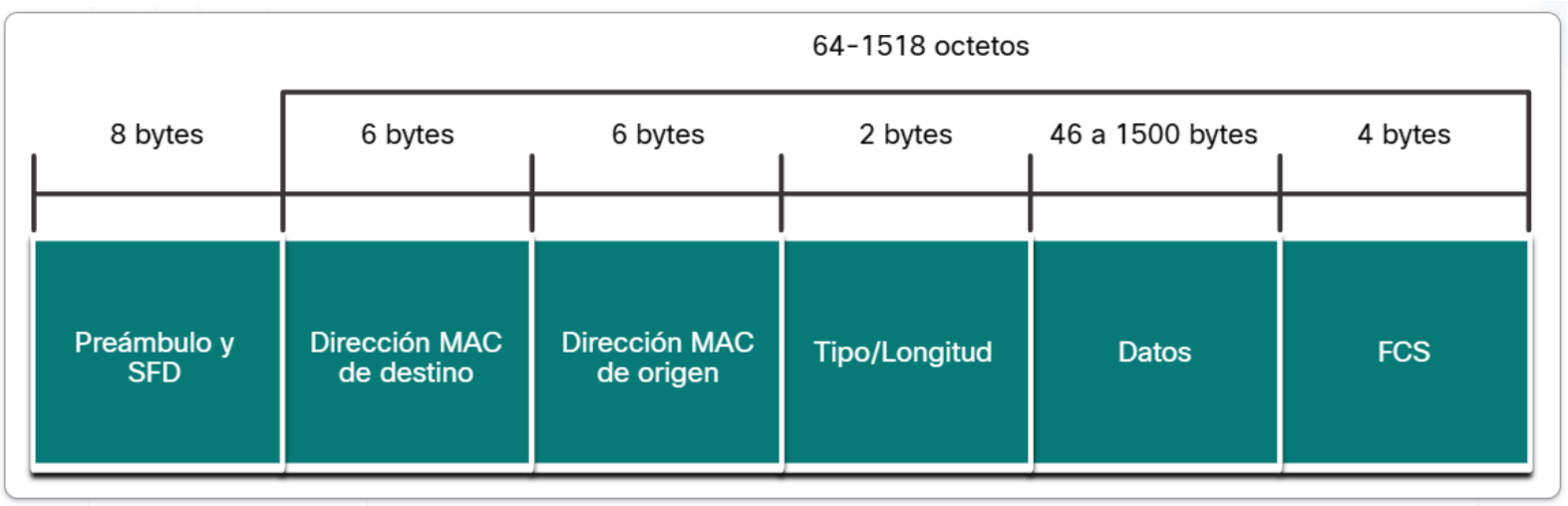
Nota: El tamaño de la trama puede ser mayor si se incluyen requisitos adicionales, como el etiquetado de VLAN. El etiquetado de VLAN está fuera del alcance de este curso.

Cualquier trama de menos de 64 bytes de longitud se considera un fragmento de colisión o una trama corta, y es descartada automáticamente por las estaciones receptoras. Las tramas de más de 1500 bytes de datos se consideran “jumbo” o "tramas bebés gigantes".

Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es posible que las tramas descartadas se originen en colisiones u otras señales no deseadas. Ellas se consideran inválidas. Las tramas jumbo suelen ser compatibles con la mayoría de los conmutadores Fast Ethernet y Gigabit Ethernet, y las NICs.

La figura muestra cada campo en la trama Ethernet. Consulte la tabla para obtener más información sobre la función de cada campo.

Campos de la Trama de Ethernet



CAMPO	DESCRIPCION
Preámbulo/SFD	Campo de 8 bytes: el Preámbulo (7 primeros bytes) y el SFD o delimitador de inicio de trama (1 byte final). Se utilizan para la sincronización entre el dispositivo emisor y receptor. Indican al receptor que se prepare para recibir una nueva trama.

Dirección MAC destino	Campo de 6 bytes, identifica la MAC del destinatario. La capa 2 de los dispositivos usan esta dirección para compararlas con su MAC y así determinar si la trama está dirigida a ellos.
Dirección MAC origen	Campo de 6 bytes, identifica la interfaz o NIC de origen de la trama.
Tipo/Longitud o EtherType	Campo de 2 bytes, identifica el protocolo de capa superior encapsulado en la trama de Ethernet. Para IPv4 es 0X800, para IPv6 es 0X86DD, para ARP es 0X806.
Datos	Campo de 46 a 1500 bytes, contiene los datos encapsulados de una capa superior. Es un paquete IPv4 o PDU capa 3. En este campo se usa un pad de relleno cuando la trama es menor de 64 bytes de longitud.
FCS	Campo secuencia de verificación de trama de 4 bytes, detecta errores en la trama, para ello el dispositivo emisor hace una **Comprobación Cíclica De Redundancia** (**CRC)** y la incluye en la trama. El receptor la recibe y genera una CRC para buscar errores. Si hay coincidencia, no hubo errores, de lo contrario se descarta la trama.

4.2.5 Verifique su Comprensión - La Trama Ethernet

¿Qué parte de una trama Ethernet utiliza un pad para aumentar el campo de trama a al menos 64 bytes?

EtherType	Preámbulo	Delimitador de inicio de trama	Campo de datos ☺←

Todas las tramas deben tener, al menos, 64 bytes de longitud. Los bits adicionales llamados "pad" se utilizan para aumentar el tamaño de la trama al tamaño mínimo.

¿Qué parte de una trama Ethernet detecta errores en la trama?

Preámbulo	Delimitador de inicio de trama	Secuencia de verificación de trama ☺←

El campo FCS utiliza un CRC para detectar errores en una trama.

¿Cuál parte de una trama Ethernet describe el protocolo de capa superior que está encapsulado?

EtherType ☺←	Preámbulo	Delimitador de inicio de trama	Secuencia de verificación de trama

El campo EtherType identifica el protocolo de capa superior encapsulado en la trama de Ethernet.

¿Qué parte de una trama Ethernet notifica al receptor que se prepare para una nueva trama?

Delimitador de inicio de trama	Secuencia de verificación de trama	Preámbulo ☺←	Campo de datos

Los primeros bytes del preámbulo informan al receptor de un nuevo trama.

¿Qué subcapa de enlace de datos controla la interfaz de red a través de controladores de software?

MAC	LLC ☺←

La subcapa LLC es responsable de controlar la tarjeta de interfaz de red a través de controladores de software.

¿Qué subcapa de enlace de datos funciona con las capas superiores para agregar información de la aplicación para la entrega de datos a protocolos de nivel superior?

MAC	LLC ☺←

La LLC trabaja con capas superiores para admitir protocolos de nivel superior.

¿Cuáles son funciones de la subcapa MAC? (Elija tres opciones).

Control de acceso a los medios ☺←	Comprueba si hay errores en los bits recibidos ☺←	Utiliza CSMA/CD o CSMA/CA para admitir la tecnología Ethernet ☺←
Se comunica entre el software en las capas superiores y el hardware del dispositivo en las capas inferiores	Permite que múltiples protocolos de Capa 3 utilicen la misma interfaz de red y medios	

La subcapa MAC comprueba si hay errores de bits, admite tecnologías Ethernet y controla el acceso a los medios.

4.2.6 Laboratorio - Visualización del Tráfico Capturado en Wireshark

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Descargar e instalar Wireshark
- Capturar y analizar datos de ARP en Wireshark
- Ver las entradas de la caché ARP en la PC.

Topología

Objetivos

Parte 1: Descargar e instalar Wireshark

Parte 2: Capturar y analizar datos de ARP en Wireshark

- Inicie y detenga la captura de datos del tráfico de ping a los hosts remotos.
- Localice la información de las direcciones IPv4 y MAC en las PDU capturadas.
- Analice el contenido de los mensajes ARP intercambiados entre los dispositivos en la LAN.

Parte 3: Ver las entradas de caché ARP en la PC

- Acceder a la línea de comandos de Windows.
- Use el comando *arp* de Windows para ver la caché de la tabla ARP local en la PC.

Aspectos básicos/situación

TCP/IP usa el protocolo de resolución de direcciones (ARP) para asignar una dirección IPv4 de capa 3 a una dirección MAC de capa 2. Cuando se transmite una trama Ethernet en la red, debe tener una dirección MAC de destino. Para detectar dinámicamente la dirección MAC de un destino conocido, el dispositivo de origen difunde una solicitud ARP en la red local. El dispositivo que está configurado con la dirección IPv4 de destino responde la solicitud con una respuesta ARP y la dirección MAC se registra en la caché ARP.

Cada dispositivo de la LAN mantiene su propia caché ARP. La caché ARP es un área pequeña en la RAM que conserva las respuestas ARP. Al abrir la caché ARP de una PC se puede ver la dirección IPv4 y la dirección MAC de cada dispositivo en la LAN con el que la PC ha intercambiado mensajes ARP.

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para la solución de problemas de red, análisis, desarrollo de protocolo y software y educación. Cuando los flujos de datos van y vienen por la red, el detector "captura" cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo con las especificaciones de protocolo correspondientes.

Wireshark es una herramienta útil para cualquier persona que trabaja con redes y se puede usar con la mayoría de los laboratorios en los cursos de Cisco para realizar análisis de datos y solución de problemas. Esta práctica de laboratorio proporciona instrucciones para descargar e instalar Wireshark, aunque es posible que ya esté instalado. En este laboratorio, usará Wireshark para capturar intercambios ARP en la red local.

Recursos necesarios

- 1 PC (Windows 10)
- Acceso a Internet
- Se usarán PC adicionales en una red de área local (LAN) para responder las solicitudes **ping**. Si no hay PC adicionales en la LAN, la dirección de la puerta de enlace predeterminada se usará para responder las solicitudes **ping**.

Instrucciones

Parte 1: Descargar e instalar Wireshark

Wireshark se convirtió en el programa detector de paquetes estándar del sector que utilizan los ingenieros de redes. Este software de código abierto está disponible para muchos sistemas operativos diferentes, incluidos Windows, MAC y Linux.

Si Wireshark ya está instalado en la PC, puede omitir la parte 1 e ir directamente a la parte 2. Si Wireshark no está instalado en la PC, consulte con el instructor acerca de la política de descarga de software de la academia.

Paso 1: Descargue Wireshark.

a. Wireshark se puede descargar de www.wireshark.org.
b. Haga clic en **Download** (Descargar).
c. Elija la versión de software que necesita según la arquitectura y el sistema operativo de la PC. Por ejemplo, si tiene una PC de 64 bits con Windows, seleccione **Instalador de Windows (64 bits)** (Windows Installer (64-bit)).
d. Después de realizar la selección, la descarga debería comenzar. Haga clic en **Guardar archivo**, si aparece un mensaje de confirmación. La ubicación del archivo descargado depende del navegador y del sistema operativo que utiliza. Para usuarios de Windows, la ubicación predeterminada es la carpeta **Descargas** (Downloads).

Paso 2: Instale Wireshark.

a. El archivo descargado se denomina **Wireshark-win64-x.x.x.exe**, en el que **x** representa el número de versión. Haga doble clic en el archivo para iniciar el proceso de instalación.
b. Responda los mensajes de seguridad que aparezcan en la pantalla. Si ya tiene una copia de Wireshark en la PC, puede que se le solicite desinstalar la versión anterior antes de instalar la versión nueva. Se recomienda eliminar la versión anterior de Wireshark antes de instalar otra versión. Haga clic en **Sí** para desinstalar la versión anterior de Wireshark.
c. Si es la primera vez que instala Wireshark, o si lo hace después de haber completado el proceso de desinstalación, navegue hasta el asistente para instalación de Wireshark. Haga clic en **Siguiente**.
d. Continúe avanzando por el proceso de instalación. Cuando aparezca la ventana Acuerdo de licencia, haga clic en **Acepto**.
e. Guarde la configuración predeterminada en la ventana Elegir componentes y haga clic en **Siguiente**.
f. Elija las opciones de método abreviado que desee y, a continuación, haga clic en **Siguiente**.
g. Puede cambiar la ubicación de instalación de Wireshark, pero, a menos que tenga un espacio en disco limitado, se recomienda mantener la ubicación predeterminada.
h. Para capturar datos de red en vivo, Npcap debe estar instalado en su PC. Si su versión instalada de Npcap es anterior a la versión que viene con Wireshark, se recomienda que permita que se instale la versión más nueva haciendo clic en la **casilla de verificación Install Npcap x.x.x** (número de versión). Haga clic en **Siguiente**.
i. Se abre una ventana independiente para la configuración de Npcap. Cuando aparezca la ventana Acuerdo de licencia, haga clic en **Acepto**. En la ventana Opciones de instalación, deje todas las casillas de verificación sin seleccionar y haga clic en **Instalar** para instalar Npcap. Haga clic en **Next** (Siguiente) cuando termine. Haga clic en **Finish** (Finalizar) para salir del asistente.
j. La instalación de USBPcap no es necesaria para este curso. Solo es necesario si planea capturar el tráfico USB. Haga clic en **Install** (Instalar) para iniciar la instalación. **Nota**: **Dado que USBPcap es experimental, asegúrese de haber creado un punto de restauración del sistema antes de la instalación de USBPcap.**
k. Wireshark comienza a instalar los archivos, y aparece una ventana independiente con el estado de la instalación. Haga clic en **Siguiente** cuando finalice la instalación.
l. Haga clic en **Finalizar** para completar el proceso de instalación de Wireshark. Si el proceso de instalación está detenido, verifique que la instalación de Npcap haya finalizado. Haga clic en **Next** (Siguiente) para continuar.
m. Reinicie la PC para finalizar la instalación.

Parte 2: Capturar y analizar los datos ARP locales en Wireshark

En la parte 2 de este laboratorio, hará ping a otra PC de la LAN y capturará las solicitudes y respuestas ARP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes para transmitir datos al destino.

Paso 1: Recupere las direcciones de interfaz de la PC.

Para este laboratorio, deberá conocer la dirección IPv4 y la dirección MAC de la PC.

a. Navegue a una ventana de línea de comandos, escriba **ipconfig /all** en el indicador.

b. Observe qué adaptador de red está usando la PC para acceder a la red. Registre la dirección IPv4 y la dirección MAC (dirección física) de la interfaz de la PC.

```
C:\Users\Student> ipconfig /all
<output omitted>
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix. :
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
   Physical Address. . . . . . . . . : A4-AE-31-AD-78-4C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f9e7:e41d:a772:f993%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, August 04, 2016 05:35:35 PM
   Lease Expires . . . . . . . . . . : Friday, August 05, 2016 05:35:35 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 245648945
   DHCPv6 IAID . . . . . . . . . . . : 00-01-00-01-1B-87-BF-52-A4-4E-31-AD-78-4C
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

c. Pida a un miembro del equipo la dirección IPv4 de su PC y dígale a esa persona la dirección IPv4 de la PC que usted está usando. En esta instancia, no proporcione su dirección MAC.

Registre las direcciones IPv4 de la puerta de enlace predeterminada y las otras PC de la LAN.

Paso 2: Inicie Wireshark y comience a capturar datos

a. En su PC, haga clic en **Inicio** y escriba **Wireshark.** Haga clic en **Wireshark Desktop App** cuando aparezca en la ventana de los resultados de la búsqueda.
Nota: De manera alternativa, es posible que su instalación de Wireshark también le dé la opción Wireshark Legacy. Esto muestra Wireshark en la GUI anterior, más antigua pero bien conocida. El resto de este laboratorio se realizó con la GUI de Desktop App más nueva.

b. Después de que se inicie Wireshark, seleccione la interfaz de red que identificó con el comando **ipconfig**. Escriba **arp** en el cuadro del filtro. Esta selección configura Wireshark para que solo muestre los paquetes que son parte de los intercambios ARP entre los dispositivos de la red local. Una vez que haya seleccionado la interfaz correcta e ingresado la información del filtro, haga clic en **Comenzar** a capturar paquetes (icono de aleta de tiburón) para comenzar la captura de datos.
La información comienza a desplazar hacia abajo la sección superior de Wireshark. Cada línea representa un mensaje que se está enviando entre un dispositivo de origen y uno de destino en la red.

c. En una ventana de línea de comandos, haga ping en la puerta de enlace predeterminada para probar la conectividad con la dirección de la puerta de enlace predeterminada que se identificó en la Parte 2, Paso 1.

```
C:\Users\Student> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=7ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 7ms, Average = 4ms
```

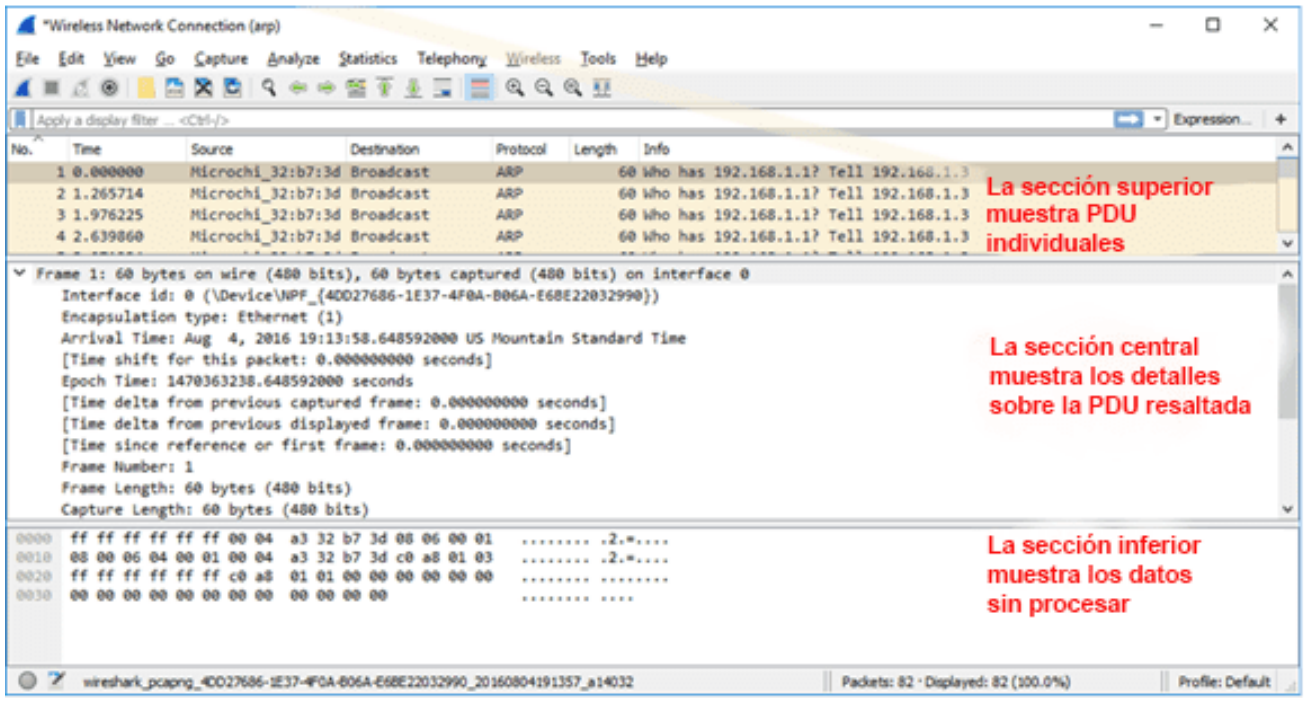
d. Envíe un comando ping a las direcciones IPv4 de las otras PC de la LAN que le proporcionaron a usted los miembros de su equipo.
Nota: Si la PC del miembro del equipo no responde a sus pings, es posible que se deba a que el firewall de la PC está bloqueando estas solicitudes. Pida ayuda al instructor si es necesario deshabilitar el firewall de la PC.

e. Deje de capturar datos haciendo clic en **Detener captura** (Stop Capture) (icono de cuadrado rojo) en la barra de herramientas.

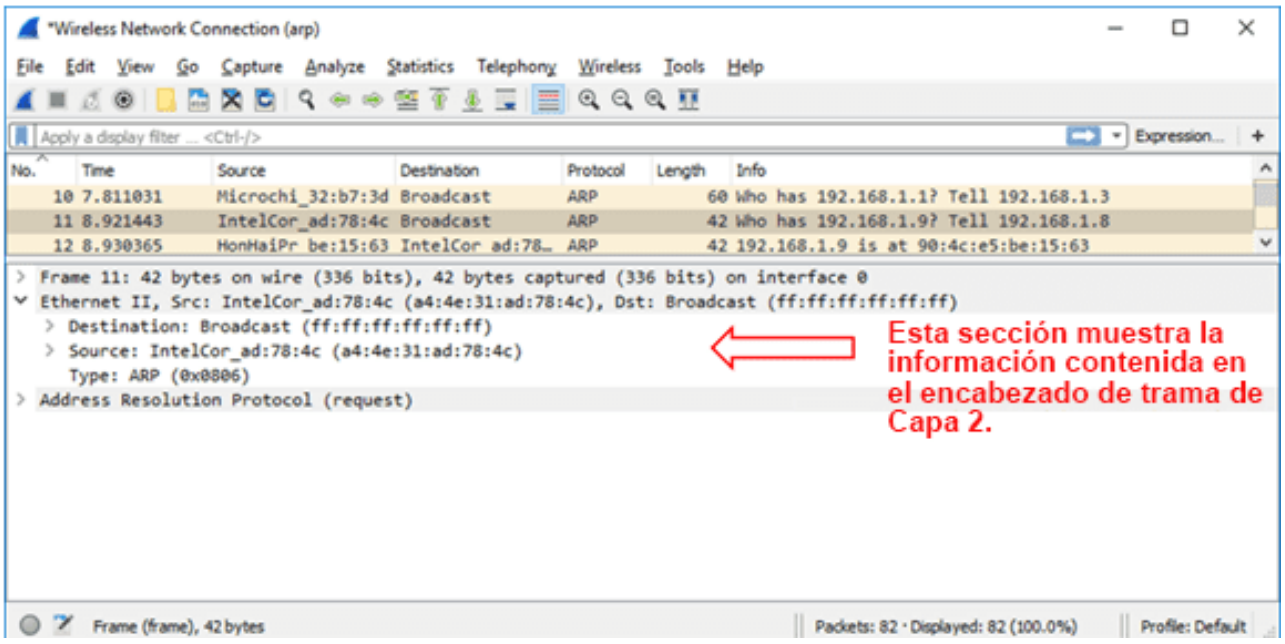
Paso 3: Examine los datos capturados

En el paso 3, examine los datos que generaron las solicitudes **ping** de la PC del miembro de su equipo. Los datos de Wireshark se muestran en tres secciones:

1) La sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IPv4.
2) La sección del medio muestra la información de PDU de la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas del protocolo.
3) La sección inferior muestra los datos de cada capa sin formato. Los datos sin procesar se muestran en formatos hexadecimal y decimal.

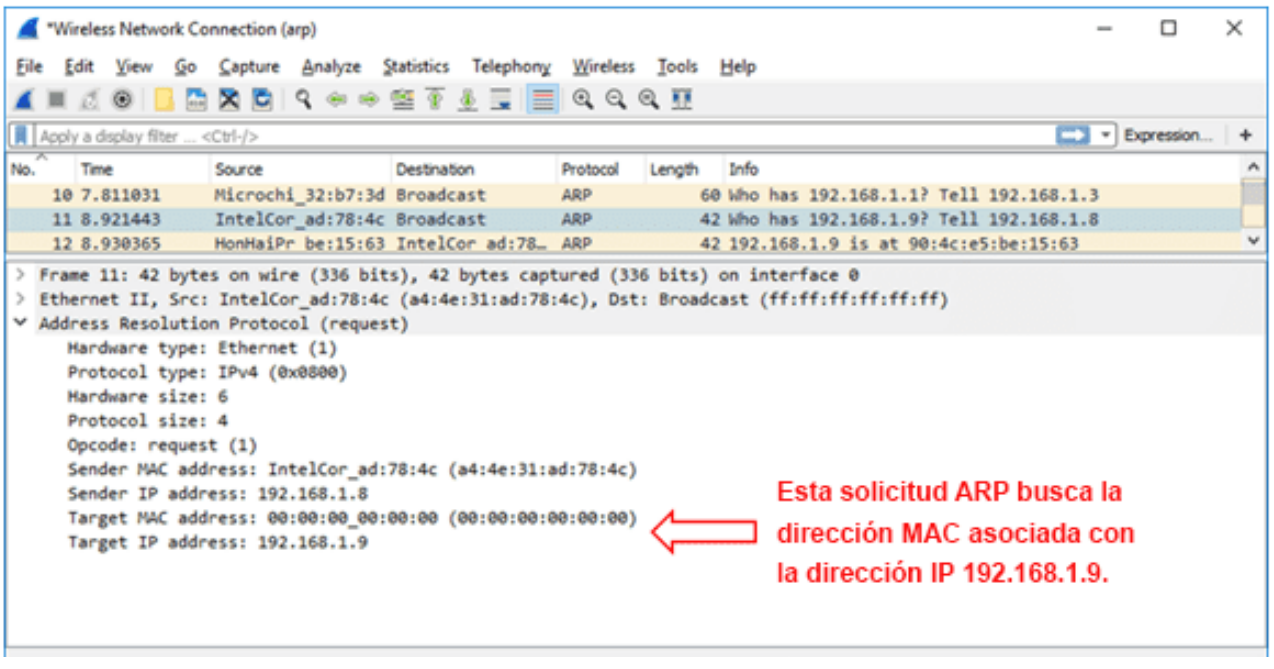


a. Haga clic en una de las tramas ARP de la parte superior que tenga la dirección MAC de la PC como dirección de origen en la trama y “difusión” como el destino de la trama.
b. Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la sección media. Haga clic en la flecha que se encuentra a la izquierda de la fila Ethernet II para ver las direcciones MAC de origen y de destino.



¿La dirección MAC de origen coincide con la interfaz de su PC? *Sí, debe coincidir con su dirección MAC*.

c. Haga clic en la flecha que se encuentra a la izquierda de la fila Protocolo de resolución de direcciones (solicitud) para ver el contenido de la solicitud ARP.



Paso 4: Localice la trama de respuesta ARP que corresponde a la solicitud ARP que seleccionó.

a. Con la dirección IPv4 de destino en la solicitud ARP, localice la trama de respuesta ARP en la sección superior de la pantalla de la captura de Wireshark. ¿Cuál es la dirección IPv4 del dispositivo de destino de su solicitud ARP?
b. Seleccione la trama de respuesta en la sección superior del resultado de Wireshark. Es posible que deba desplazarse por la ventana para encontrar la trama de respuesta que coincida con la dirección IPv4 de destino identificada en el paso anterior. Expanda las filas Ethernet II y Address Resolution Protocol (Protocolo de resolución de direcciones) (respuesta) en la sección del medio de la pantalla. ¿La trama de respuesta ARP es una trama de difusión? Rpta: No. ¿Cuál es la dirección MAC de destino de la trama? ¿Es la dirección MAC de su PC? Rpta: Si. ¿Qué dirección MAC es el origen de la trama?
c. Verifique con el miembro de su equipo que la dirección MAC coincida con la dirección de la PC.

Parte 3: Examine las entradas de la caché ARP en la PC.

Después de recibir la respuesta ARP en la PC, la asociación de la dirección MAC con la dirección IPv4 se almacena en la memoria caché en la PC. Estas entradas permanecerán en la memoria por un breve período (de 15 a 45 segundos); luego, si no se usan durante ese período, se borran de la caché.

a. Abra una ventana de línea de comandos en la PC. En la línea de comandos, escriba **arp –a** y presione Enter.

C:\Users\Student> **arp -a**

```
Interface: 192.168.1.8 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           00-37-73-ea-b1-7a     dynamic
  192.168.1.9           90-4c-e5-be-15-63     dynamic
  192.168.1.13          a4-4e-31-ad-78-4c     dynamic
  224.0.0.5             01-00-5e-00-00-05     static
  224.0.0.6             01-00-5e-00-00-06     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

El resultado del comando **arp –a** son las entradas que se encuentran en la caché de la PC. En el ejemplo, la PC tiene entradas para la puerta de enlace predeterminada (192.168.1.1) y para dos PC que se encuentran en la misma LAN (192.168.1.9 y 192.168.1.13).

¿Qué produce el arp –a en su PC? *Rpta: Las respuestas varían, pero el comando enumera las asignaciones de direcciones MAC a IPv4 conocidas.*

b. El comando ***arp*** en la PC con Windows tiene otra función. Ingrese arp /? en la línea de comando y presione Enter (Intro). Las opciones del comando arp le permiten ver, agregar y eliminar las entradas de la tabla ARP si es necesario.

¿Qué opción elimina una entrada de la caché ARP? Rpta: arp -d. ¿Cuál sería el resultado del comando arp –d *? Eliminaría las asignaciones de direcciones actuales en la caché ARP. Este comando requiere privilegios administrativos en Windows 10.

1. ¿Cuál es el beneficio de mantener las entradas de la caché ARP en memoria en la computadora de origen?

Rpta: Su computadora revisa siempre su caché local antes de solicitar información de otros dispositivos en la red. La caché ARP retiene las asociaciones de direcciones obtenidas dinámicamente correspondientes a un período breve. Cuando se intercambia tráfico a menudo entre el origen y el destino, la caché ARP evita que el host difunda solicitudes ARP innecesariamente.

2. Si la dirección IPv4 de destino no se encuentra en la misma red que el host de origen, ¿qué dirección MAC se usará como dirección MAC de destino en la trama?

Rpta: La computadora usará la dirección MAC de la puerta de enlace predeterminada.

4.2.7 Laboratorio - Uso de Wireshark para Examinar Tramas Ethernet

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Examinar los campos de encabezado de una trama de Ethernet II
- Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

Aspectos básicos/situación

Cuando los protocolos de capa superior se comunican entre sí, los datos fluyen por las capas de interconexión de sistemas abiertos (OSI) y se encapsulan en una trama de capa 2. La composición de la trama depende del tipo de acceso al medio. Por ejemplo, si los protocolos de capa superior son TCP e IP, y el acceso a los medios es Ethernet, el encapsulamiento de tramas de capa 2 es Ethernet II. Esto es típico para un entorno LAN. Al aprender sobre los conceptos de la capa 2, es útil analizar la información del encabezado de la trama. En la Parte 1, revisará los campos que contiene una trama de Ethernet II. En la Parte 2, utilizará Wireshark para capturar y analizar campos de encabezado de tramas de Ethernet II de tráfico local y remoto.

Recursos necesarios

- 1 PC (opción de sistema operativo con Wireshark instalado)
- Acceso a Internet

Instrucciones

Parte 1: Examinar los campos de encabezado de una trama de Ethernet II

En esta parte, examinará los campos de encabezado y el contenido de una trama Ethernet II. Se utilizará una captura de Wireshark para examinar el contenido de esos campos.

Paso 1: Revisar las descripciones y longitudes de los campos de encabezado de Ethernet II

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

Paso 2: Examinar la configuración de red de la PC

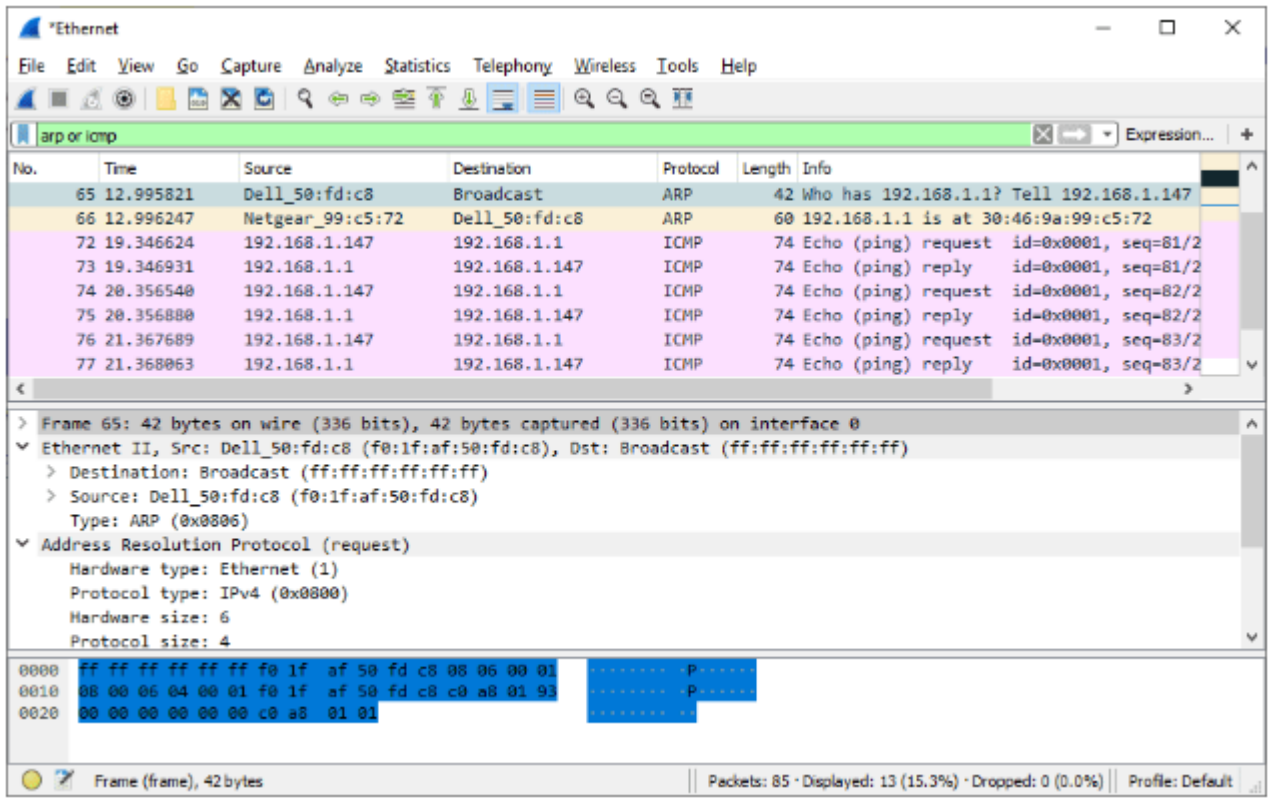
En este ejemplo, la dirección IP del host de esta PC es 192.168.1.147 y la puerta de enlace predeterminada tiene una dirección IP de 192.168.1.1. (Para Linux y MAC OS, utilice el comando ipconfig en la terminal).

```
C:\> ipconfig /all

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix. :
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection
   Physical Address. . . . . . . . . : F0-1F-AF-50-FD-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . .: fe80: :58c 5:45 f 2:7 e5e:29c 2% 11 (Preferido)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : viernes 6 de septiembre de 2019 11:08:36
   Lease Expires . . . . . . . . . . : sábado 7 de septiembre de 2019 11:08:36
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
<output omitted>
```

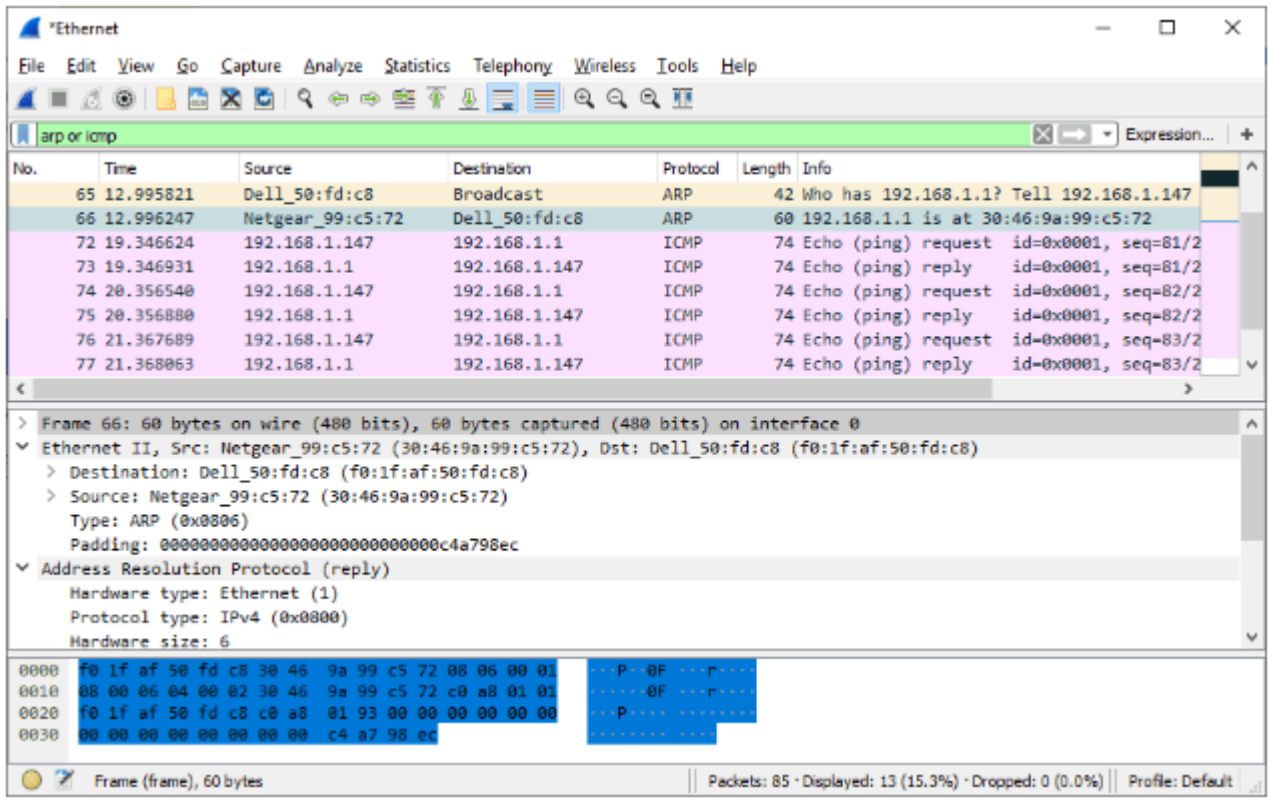
Paso 3: Examinar las tramas de Ethernet en una captura de Wireshark

Las imágenes de la captura de Wireshark a continuación muestran los paquetes generados por un ping emitido desde un host de PC a su puerta de enlace predeterminada. Se aplicó un filtro (arp o icmp) a Wireshark para ver solo los protocolos ARP e ICMP. ARP significa protocolo de resolución de direcciones. ARP es un protocolo de comunicación que se utiliza para determinar la dirección MAC asociada a la dirección IP. La sesión comienza con una consulta ARP para obtener la dirección MAC del router de la puerta de enlace seguida de cuatro solicitudes y respuestas de ping.

Esta captura de pantalla resalta los detalles del fotograma de una solicitud ARP.



Esta captura de pantalla resalta los detalles de la trama para una respuesta ARP.



Paso 4: Examinar el contenido del encabezado de Ethernet II de una solicitud de ARP

En la siguiente tabla, se toma la primera trama de la captura de Wireshark y se muestran los datos de los campos de encabezado de Ethernet II.

Campo	Valor	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de la NIC.
Dirección de destino	Broadcast (ff:ff:ff:ff:ff:ff) (Difusión [ff:ff:ff:ff:ff:ff])	Direcciones de capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o 6 octetos, expresada como 12 dígitos hexadecimales (`0-9, A-F`). Un formato común es `12:34:56:78:9A:BC`.
Dirección de origen	NetGear_99:C 5:72 (30:46:9 a:99:c 5:72)	Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC), y los últimos seis números son el número de serie de la NIC. La dirección de destino puede ser de difusión, que contiene todos números uno, o de unidifusión. La dirección de origen siempre es de unidifusión.
Tipo de trama	0x0806	Para las tramas de Ethernet II, este campo contiene un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior del campo de datos. Ethernet II admite varios protocolos de capa superior. Dos tipos comunes de trama son los siguientes: Valor Descripción `0x0800` Protocolo IPv4 `0x0806` Protocolo de resolución de direcciones (ARP)
Datos	ARP	Contiene el protocolo de nivel superior encapsulado. El campo de datos tiene entre 46 y 1500 bytes.
FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El equipo emisor calcula el valor abarcando las direcciones de trama, campo de datos y tipo. El receptor lo verifica.

¿Qué característica significativa tiene el contenido del campo de dirección de destino?

Todos los hosts de la LAN reciben esta trama de difusión. El host que tiene la dirección IP 192.168.1.1 (gateway predeterminado) envía una respuesta de unidifusión al origen (equipo host). Esta respuesta contiene la dirección MAC de la NIC del gateway predeterminado.

¿Por qué envía la PC un ARP de difusión antes de enviar la primera solicitud de ping?

La PC no puede enviar una solicitud de ping a un host hasta que determine la dirección MAC de destino, de modo que pueda crear el encabezado de la trama para esa solicitud de ping. La difusión de ARP se utiliza para solicitar la dirección MAC del host con la dirección IP incluida en el ARP.

¿Cuál es la dirección MAC del origen en la primera trama? Varía; en este caso, es f 0:1 f:af:50:fd:c8.

¿Cuál es el ID de proveedor (OUI) de la NIC de origen en la respuesta ARP? Varía, en este caso, es Dell.

¿Qué porción de la dirección MAC corresponde al OUI? Los primeros 3 octetos de la dirección MAC indican el OUI.

¿Cuál es el número de serie de la NIC del origen? Puede variar, en este caso es 99:c5:72.

Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet
En esta parte, utilizará Wireshark para capturar tramas de Ethernet locales y remotas. Luego, examinará la información que contienen los campos de encabezado de las tramas.

Paso 1: Determinar la dirección IP del gateway predeterminado de la PC
Abra una ventana del símbolo del sistema y emita el comando ipconfig. (Para Linux y MAC OS, introduzca el comando netstat -rn en una terminal).
Registre la dirección IP de la puerta de enlace predeterminada de la PC.

Paso 2: Comenzar a capturar el tráfico de la NIC de la PC

a. Abrir Wireshark para iniciar la captura de datos. Haga doble clic en la interfaz del dispositivo de red deseado con tráfico de red para iniciar la captura.
b. Observe el tráfico que aparece en la ventana Packet List (Lista de paquetes).

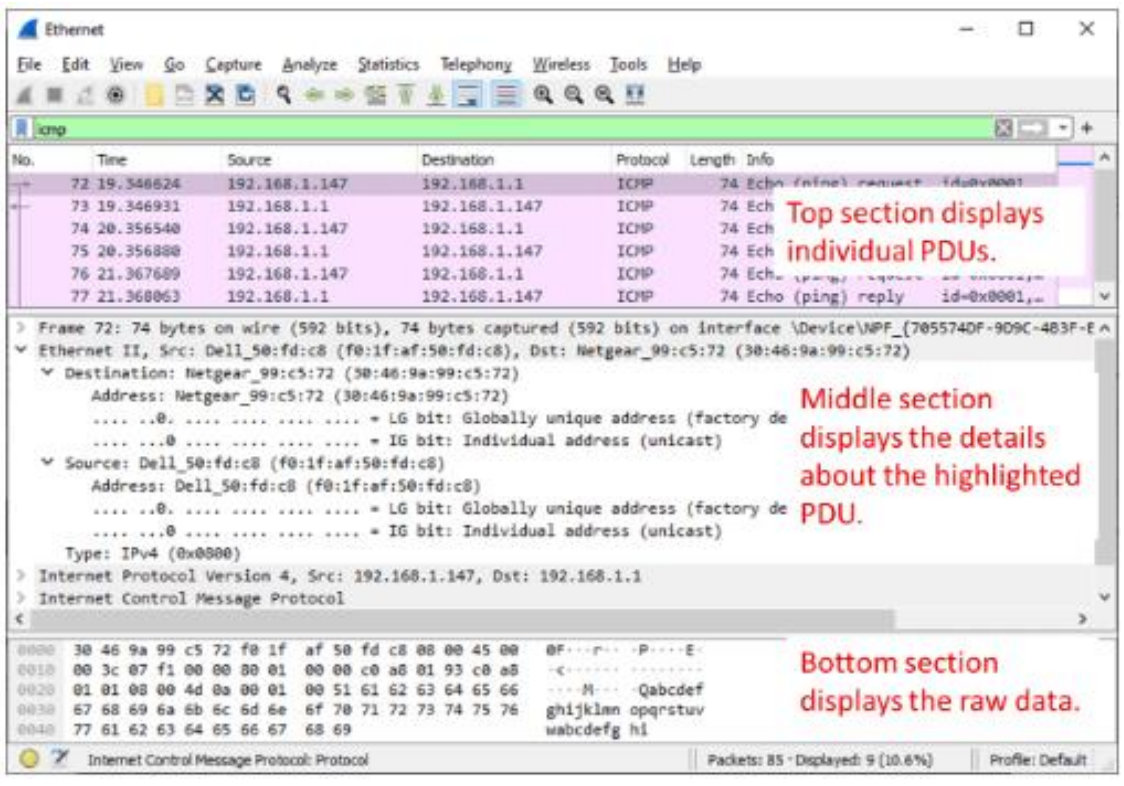
Paso 3: Filtrar Wireshark para que solamente se muestre el tráfico ICMP
Puede usar el filtro de Wireshark para bloquear la visibilidad del tráfico no deseado. El filtro no bloquea la captura de datos no deseados; solo filtra lo que desea mostrar en la pantalla. Por el momento, solo se debe visualizar el tráfico ICMP.
En el cuadro Filter (Filtro) de Wireshark, escriba icmp. Si escribió el filtro correctamente, el cuadro debe volverse de color verde. Si el cuadro está de color verde, haga clic en Apply (Aplicar) (la flecha hacia la derecha) para que se aplique el filtro.

Paso 4: En la ventana del símbolo del sistema, hacer un ping al gateway predeterminado de la PC
Abra una ventana de intérprete de comandos de Windows
En la ventana del símbolo del sistema, haga un ping a la puerta de enlace predeterminada con la dirección IP registrada en el Paso 1.

Cierre el símbolo del sistema de Windows.

Paso 5: Dejar de capturar el tráfico de la NIC
Haga click en el ícono de Detener Captura de Paquetes (el cuadro rojo) para detener la captura de tráfico

Paso 6: Examinar la primera solicitud de eco (ping) en Wireshark.
La ventana principal de Wireshark se divide en tres secciones: el panel Packet List (Lista de paquetes) en la parte superior, el panel Packet Details (Detalles del paquete) en la parte central y el panel Packet Bytes (Bytes del paquete) en la parte inferior. Si seleccionó la interfaz correcta para la captura de paquetes anteriormente, Wireshark debería mostrar la información ICMP en el panel de la lista de paquetes de Wireshark.



a. En el panel Packet List (Lista de paquetes) de la parte superior, haga clic en la primera trama de la lista. Debería ver el texto **Echo (ping) request (Solicitud de eco [ping])** debajo del encabezado **Info (Información)**. La línea debe resaltarse ahora.

b. Examine la primera línea del panel Packet Details (Detalles del paquete) de la parte central. Esta línea muestra la longitud de la trama.

c. En la segunda línea del panel Packet Details (Detalles del paquete), se muestra que es una trama de Ethernet II. También se muestran las direcciones MAC de origen y de destino.

¿Cuál es la dirección MAC de la NIC de la PC? Tus respuestas variarán. En este ejemplo, la dirección MAC de la PC es f0:1f:af:50:fd:c8.

¿Cuál es la dirección MAC de la puerta de enlace predeterminada? Tus respuestas variarán. En este ejemplo, la dirección MAC de la puerta de enlace predeterminada es 30:46.9a:99:c5:72.

d. Puede hacer clic en el signo mayor que (>) al comienzo de la segunda línea para obtener más información sobre la trama de Ethernet II. ¿Qué tipo de trama se muestra? Rpta: 0x0800 o un tipo de trama IPv4

e. En las últimas dos líneas de la parte central, se proporciona información sobre el campo de datos de la trama. Observe que los datos contienen información sobre las direcciones IPv4 de origen y de destino.

¿Cuál es la dirección IP de origen? Tus respuestas variarán. En este ejemplo, la dirección IP de origen es 192.168.1.147.

¿Cuál es la dirección IP de destino? Tus respuestas variarán. En este ejemplo, la dirección IP de origen es 192.168.1.1.

f. Puede hacer clic en cualquier línea de la parte central para resaltar esa parte de la trama (hexadecimal y ASCII) en el panel Packet Bytes (Bytes del paquete) de la parte inferior. Haga clic en la línea Internet Control Message Protocol (Protocolo de mensajes de control de Internet) de la parte central y examine lo que se resalta en el panel Packet Bytes (Bytes de paquete).

¿Qué texto muestran los últimos dos octetos resaltados? Hola

g. Haga clic en la siguiente trama de la parte superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y de destino se invirtieron porque esta trama se envió desde el router del gateway predeterminado como respuesta al primer ping.

¿Qué dispositivo y qué dirección MAC se muestran como dirección de destino? Tus respuestas variarán. La dirección MAC de destino será para su PC.

Paso 7: Capturar paquetes para un host remoto.

a. Haga clic en el ícono Start Capture (Iniciar captura) para iniciar una nueva captura de Wireshark. Se muestra una ventana emergente que le pregunta si desea guardar los anteriores paquetes capturados en un archivo antes de iniciar la nueva captura. Haga clic en Continue without Saving (Continuar sin guardar).

b. En la ventana del símbolo del sistema, hacer ping a www.cisco.com

c. Dejar de capturar paquetes.

d. Examinar los nuevos datos del panel de la lista de paquetes de Wireshark.

Preguntas:

En la primera trama de solicitud de eco (ping), ¿cuáles son las direcciones MAC de origen y de destino?

Origen: Esta será la dirección MAC de la PC. Destino: Esta debería ser la dirección MAC de la Puerta de Enlace Predeterminada.

¿Cuáles son las direcciones IP de origen y de destino que contiene el campo de datos de la trama?

Origen: Esta sigue siendo la dirección IP de la PC. Destino: Esta es la dirección del servidor en www.cisco.com.

Comparen estas direcciones con las direcciones que recibió en el paso anterior. La única dirección que cambió es la dirección IP de destino. ¿Por qué cambió la dirección IP de destino mientras que la dirección MAC permaneció igual?

Las tramas de capa 2 nunca abandonan la LAN. Cuando se hace ping a un host remoto, el origen utiliza la dirección MAC del gateway predeterminado para el destino de la trama. El gateway predeterminado recibe el paquete, le quita la información de trama de capa 2 y crea un nuevo encabezado de trama con la dirección MAC del siguiente salto. Este proceso continúa de router a router hasta que el paquete llega a la dirección IP de destino.

En Wireshark, no se muestra el campo de preámbulo de un encabezado de trama. ¿Qué contiene el preámbulo?

El campo de preámbulo contiene siete octetos de secuencias alternantes de “1010” y un octeto que indica el comienzo de una trama: 10101011.

3. Dirección MAC de Ethernet

4.3.1 Dirección MAC y Hexadecimal

En redes, las direcciones IPv4 se representan utilizando el sistema numérico decimal de base diez y el sistema numérico binario de base dos. Las direcciones IPv6 y las direcciones Ethernet se representan utilizando el sistema numérico hexadecimal de base dieciséis. Para entender hexadecimal, primero debe estar muy familiarizado con binario y decimal. El sistema de numeración hexadecimal usa los números del 0 al 9 y las letras de la A a la F.

Una dirección MAC Ethernet consta de un valor binario de 48 bits. Se utiliza el hexadecimal para identificar una dirección Ethernet porque un solo dígito hexadecimal representa cuatro bits binarios. Por lo tanto, una dirección MAC Ethernet de 48 bits se puede expresar utilizando sólo 12 valores hexadecimales. La figura compara los valores decimales y hexadecimales equivalentes para el binario 0000 a 1111.

Equivalentes decimales y binarios a los valores hexadecimales del 0 al F

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Dado que 8 bits (un byte) es un método de agrupación binaria común, los números binarios del 00000000 al 11111111 se pueden representar en hexadecimal como el rango del 00 al FF, como se muestra en la figura.

Equivalentes decimales, binarios y hexadecimales seleccionados

Decimal	Binario	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

Cuando se usa hexadecimal, los ceros iniciales siempre se muestran para completar la representación de 8 bits. Por ejemplo, en la tabla, el valor binario 0000 1010 se muestra en hexadecimal como 0A. Los números hexadecimales suelen ser representados por el valor precedido por **0x** (por ejemplo, **0x73**) para distinguir entre valores decimales y hexadecimales en la documentación.

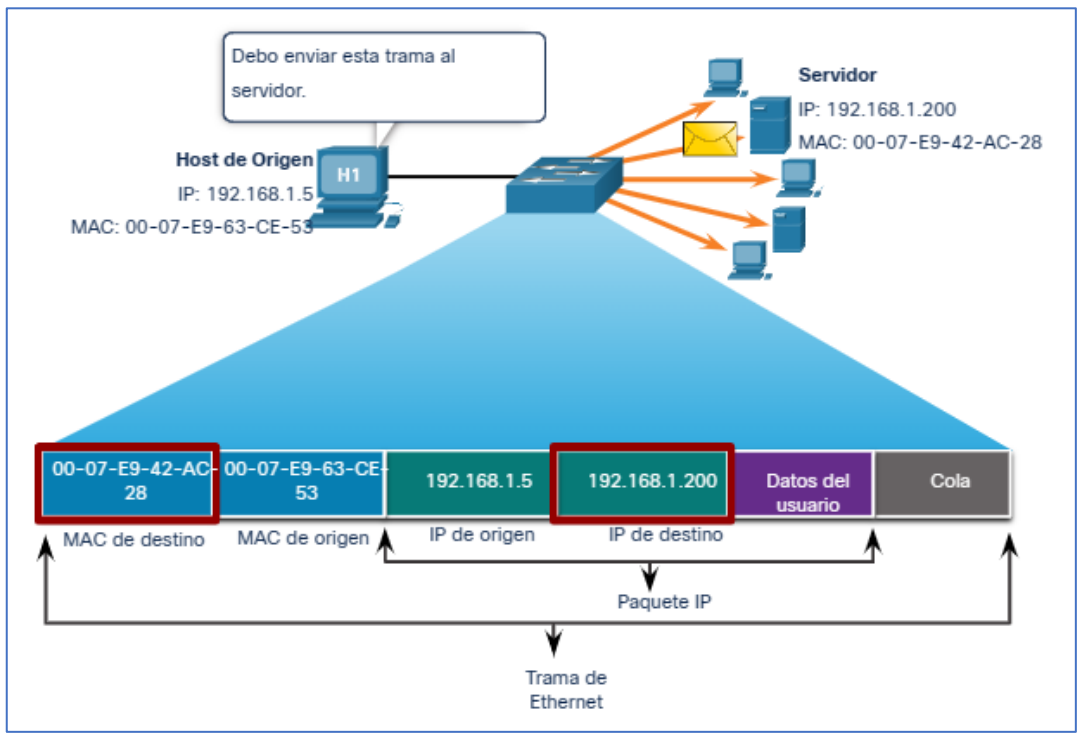
El hexadecimal también puede estar representado por un subíndice 16, o el número hexadecimal seguido de una H (por ejemplo, 73H).

Es posible que tenga que convertir entre valores decimales y hexadecimales. Si es necesario realizar dichas conversiones, generalmente, es más fácil convertir el valor decimal o hexadecimal a un valor binario y, a continuación, convertir ese valor binario a un valor decimal o hexadecimal, según corresponda.

4.3.2 Dirección MAC de Unidifusión (Unicast)

En Ethernet, se utilizan diferentes direcciones MAC para las comunicaciones de unidifusión, difusión y multidifusión de Capa 2.

Una dirección MAC de unidifusión es la dirección única que se utiliza cuando se envía una trama desde un único dispositivo de transmisión a un único dispositivo de destino.



En el ejemplo de la animación, un host con la dirección IPv4 192.168.1.5 (origen) solicita una página web del servidor en la dirección IPv4 unicast 192.168.1.200. Para que un paquete de unicast se envíe y se reciba, la dirección IP de destino debe estar incluida en el encabezado del paquete IP. Además, el encabezado de la trama de Ethernet también debe contener la dirección MAC de destino correspondiente. Las direcciones IP y MAC se requieren para la distribución de datos a un host de destino específico.

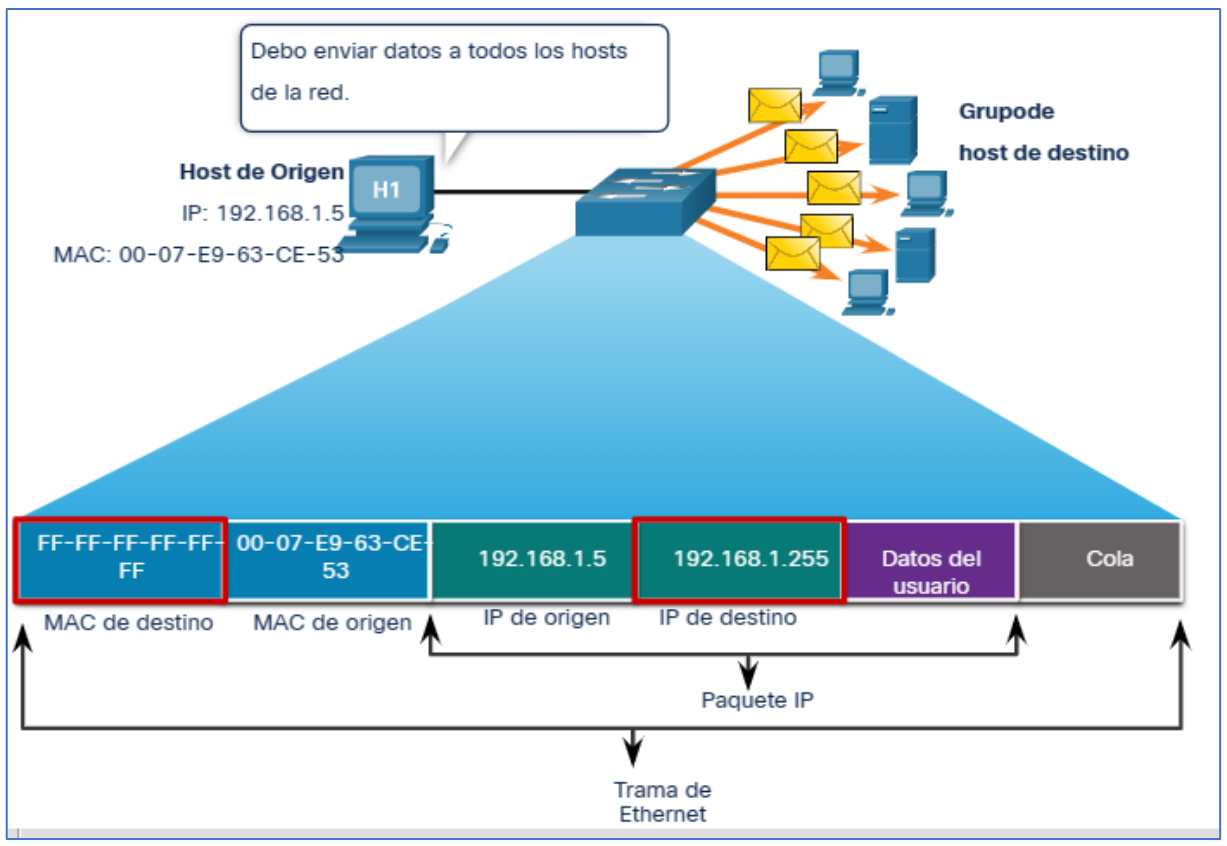
El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada a una dirección IPv4, se conoce como Protocolo de Resolución de Direcciones (ARP). El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada con una dirección IPv6 se conoce como Neighbor Discovery (ND).

Nota: La dirección MAC de origen siempre debe ser unidifusión.

4.3.3 Dirección MAC de Difusión (Broadcast)

Una trama de difusión (broadcast) de Ethernet es aquella que es recibida y procesada por cada dispositivo de la LAN Ethernet. Las características de una transmisión Ethernet son las siguientes:

- Tiene una dirección MAC de destino de **FF-FF-FF-FF-FF-FF** en hexadecimal (48 bits binarios).
- Se inunda hacia todos los puertos del conmutador Ethernet excepto el puerto entrante.
- No es reenviada por un enrutador.
- Si los datos encapsulados son un paquete de difusión IPv4, la dirección IPv4 de destino tiene todos (**1s**) en la parte del host, ello significa que todos los hosts de esa red local (dominio de difusión) recibirán y procesarán el paquete.



Como se muestra en la animación, el host de origen envía un paquete broadcast IPv4 a todos los dispositivos de la red. La dirección IPv4 de destino es una dirección broadcast: 192.168.1.255. Cuando el paquete de broadcast IPv4 se encapsula en la trama de Ethernet, la dirección MAC de destino es la dirección MAC de difusión FF-FF-FF-FF-FF-FF en hexadecimal (48 números uno en binario).

DHCP para IPv4 es un ejemplo de protocolo que utiliza direcciones de broadcast Ethernet e IPv4. Sin embargo, no todas las transmisiones Ethernet llevan un paquete de broadcast IPv4. Por ejemplo, las solicitudes ARP no utilizan IPv4, pero el mensaje ARP se envía como un broadcast Ethernet.

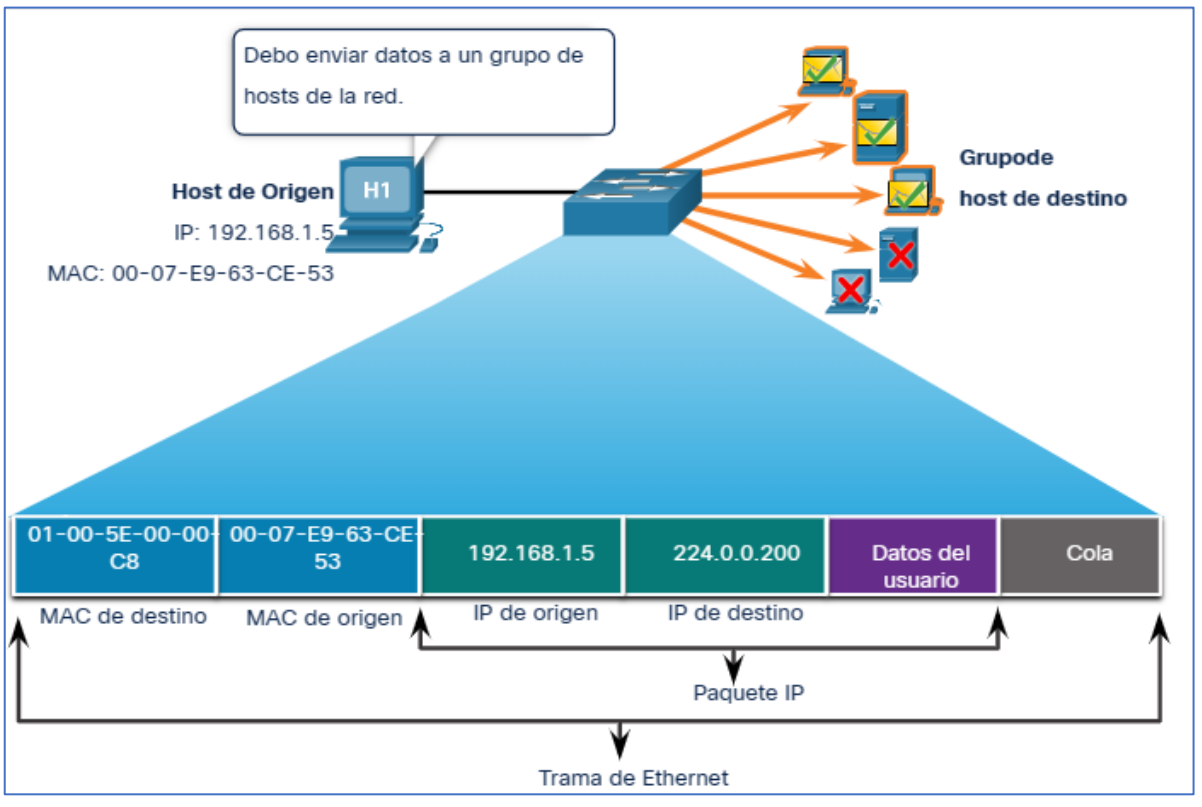
4.3.4 Dirección MAC de Multidifusión (Multicast)

Una trama multicast de Ethernet es aquella que es recibida y procesada por un grupo de dispositivos en la LAN Ethernet que pertenecen al mismo grupo de multicast. Las características de una multicast Ethernet son las siguientes:

- La dirección MAC de destino empieza con **01-00-5E** cuando los datos encapsulados son un paquete de multidifusión IPv4 y la dirección MAC de destino es **33-33** cuando los datos encapsulados son un paquete de multidifusión IPv6.
- Existen otras direcciones MAC de destino multicast reservadas para cuando los datos encapsulados no son IP, como Spanning Tree Protocol (STP) y Link Layer Discovery Protocol (LLDP).
- Se inundan todos los puertos del conmutador Ethernet excepto el puerto entrante, a menos que el conmutador esté configurado para la indagación de multidifusión.
- No es reenviado por un enrutador, a menos que el enrutador esté configurado para enrutar paquetes de multidifusión.

Si los datos encapsulados son un paquete multicast IP, a los dispositivos que pertenecen a un grupo multicast se les asigna una dirección IP de grupo multicast. El intervalo de direcciones IPv4 de multidifusión va de **224.0.0.0 a 239.255.255.255**. El rango de direcciones de multicast IPv6 comienza con **ff00::/ 8**. Debido a que las direcciones de multicast representan un grupo de direcciones (a veces denominado grupo de hosts), solo se pueden utilizar como el destino de un paquete. El origen siempre tiene una dirección de unicast.

Al igual que con las direcciones de unicast y broadcast, la dirección IP multicast requiere una dirección MAC multicast para entregar tramas en una red local. La dirección MAC multicast está asociada a la dirección multicast IPv4 o IPv6 y utiliza la información de direccionamiento de dicha dirección.



Los protocolos de enrutamiento y otros protocolos de red utilizan direccionamiento multicast. Las aplicaciones como el software de vídeo e imágenes también pueden utilizar direccionamiento multicast, aunque las aplicaciones multicast no son tan comunes.

4.3.5 Verifique su Comprensión - Dirección MAC Ethernet

¿Qué tipo de dirección MAC siguiente es dirección MAC de unidifusión?

01-00-5E-00-00-C8	00-07-E9-42-AC-28 ☺←	33-33-00-58-94-5C	FF-FF-FF-FF-FF-FF

¿Qué tipo de dirección MAC siguiente es dirección MAC de difusión?

01-00-5E-00-00-C8	00-07-E9-42-AC-28	33-33-00-58-94-5C	FF-FF-FF-FF-FF-FF ☺←

¿Qué tipo de dirección MAC siguiente es una dirección MAC de multidifusión IPv4?

01-00-5E-00-00-C8 ☺←	00-07-E9-42-AC-28	33-33-00-58-94-5C	FF-FF-FF-FF-FF-FF

¿Qué tipo de dirección MAC siguiente es una dirección MAC de multidifusión IPv6?

01-00-5E-00-00-C8	00-07-E9-42-AC-28	33-33-00-58-94-5C ☺←	FF-FF-FF-FF-FF-FF

4. La Tabla de direcciones MAC

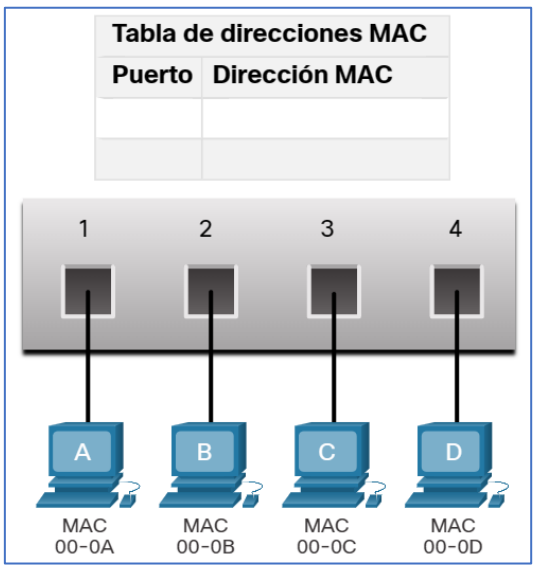
4.4.1 Fundamentos del Conmutador

Ahora que sabe todo acerca de las direcciones MAC Ethernet, es hora de hablar sobre cómo un switch utiliza estas direcciones para reenviar (o descartar) tramas a los dispositivos de una red. Si un switch reenvía cada trama que recibió a todos los puertos, su red estaría tan congestionada que probablemente se detendría por completo.

Un switch Ethernet capa 2 usa únicamente las direcciones MAC de destino para tomar decisiones de reenvío. No tiene por qué tomar conocimiento de los datos que se transportan en la trama, ya sea un paquete IPv4, un mensaje ARP o un paquete IPv6 ND. El switch toma decisiones de reenvío basándose únicamente en las direcciones MAC Ethernet de capa 2.

Un switch Ethernet examina su tabla de direcciones MAC para tomar una decisión de reenvío para cada trama, a diferencia de los hubs Ethernet heredados que repiten bits en todos los puertos excepto el puerto entrante. En la ilustración, se acaba de encender el switch de cuatro puertos. Se muestra la tabla de direcciones MAC vacía, ya que el switch aún no ha aprendido las direcciones MAC de las cuatro PC conectadas.

Nota: Las direcciones MAC se acortan a lo largo de este tema con fines de demostración.



La tabla de direcciones MAC del switch está aún vacía.

Nota: La tabla de direcciones MAC también se conoce como “**tabla CAM”** o “**tabla de Memoria de Contenido Direccionable”** (content addressable memory, CAM).

4.4.2 Aprendizaje y Reenvío del Conmutador

El conmutador arma la tabla de direcciones MAC dinámicamente, examinando las direcciones MAC origen de las tramas recibidas en un puerto. El conmutador reenvía las tramas después de buscar una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC.

Aprendizaje:

El switch revisa cada trama que ingresa a un conmutador para obtener información nueva, esto se realiza examinando la dirección MAC de origen de la trama y el número de puerto por el que ingresó al conmutador.

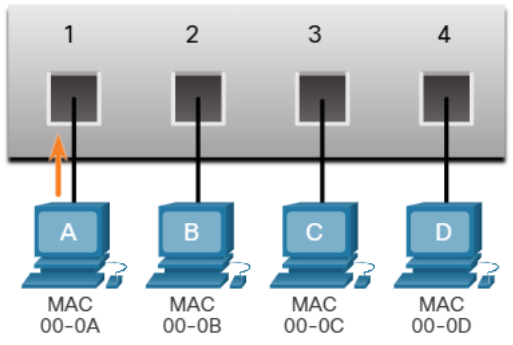
- Si la dirección MAC de origen no existe, la agrega a la tabla junto con el número de puerto de entrada.
- Si la dirección MAC de origen existe en la tabla, el conmutador actualiza el temporizador para esa entrada.
- Si la dirección MAC de origen existe en la tabla, pero en un puerto diferente, el conmutador la trata como una entrada nueva. La entrada se reemplaza con la misma dirección MAC, pero con el número de puerto más actual.

De manera predeterminada, la mayoría de los conmutadores Ethernet guardan una entrada en la tabla por cinco minutos.

En la figura, la PC-A está enviando una trama Ethernet a la PC-D. El conmutador agrega la dirección MAC de PC-A a la tabla de direcciones MAC.

1. PC-A envía una trama Ethernet.
2. El conmutador agrega el número de puerto y la dirección MAC de PC-A a su tabla de direcciones MAC.

Tabla de direcciones MAC	
Puerto	**Dirección MAC**
1	00-0A



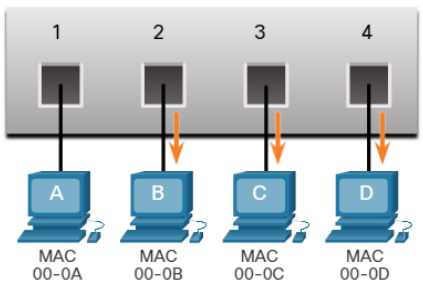
Reenvío: El switch examina la Dirección MAC de Destino

a) Si la Dirección MAC de Destino es de unidifusión, el conmutador busca una coincidencia entre la dirección MAC de destino de la trama y una entrada o registro similar en su tabla de direcciones MAC.

- Si la dirección MAC de destino está en la tabla, reenvía la trama por el puerto especificado.
- Si la dirección MAC de destino no está en la tabla, el conmutador reenvía la trama por todos los puertos, excepto el puerto de entrada. Esto se conoce como unidifusión desconocida.

b) Si la Dirección MAC de destino es de difusión o multidifusión, la trama también se envía a todos los puertos, excepto el puerto de entrada.

Tabla de direcciones MAC	
Puerto	**Dirección MAC**
1	00-0A



En la figura, PC-A envía una trama a PC-D, el switch no tiene la dirección MAC de destino en su tabla, por lo que envía la trama a todos sus puertos, excepto al puerto 1 por el que entró.

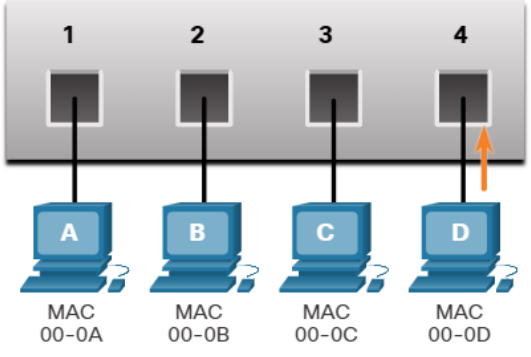
4.4.3 Filtrado de Tramas

A medida que un conmutador recibe tramas de diferentes dispositivos, puede completar la tabla de direcciones MAC examinando la dirección MAC de cada trama. Cuando la tabla de direcciones MAC del conmutador contiene la dirección MAC de destino, puede filtrar la trama y reenviarla a un solo puerto.

PC-D a Switch:

En la figura, PC-D responde a PC-A. El switch ve la dirección MAC de PC-D en la trama entrante en el puerto 4. A continuación, el switch coloca la dirección MAC de PC-D en la tabla de direcciones MAC asociada con el puerto 4. El switch agrega el número de puerto y la dirección MAC de PC-D a su tabla de direcciones MAC.

Tabla de direcciones MAC	
Puerto	**Dirección MAC**
1	00-0A
4	00-0D

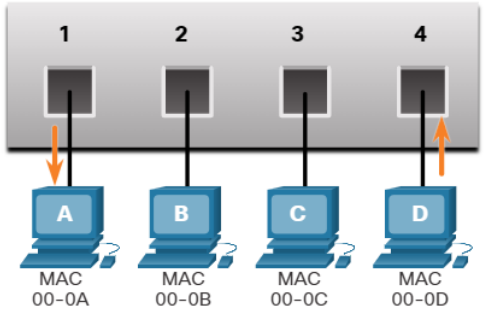


Switch a PC-A:

A continuación, dado que el switch tiene la dirección MAC de destino para la PC-A en la Tabla de direcciones MAC, enviará la trama solo al puerto 1, como se muestra en la figura.

1. El switch tiene registrada la dirección MAC para el destino.
2. El switch filtra la trama, enviándola solo por el puerto 1.

Tabla de direcciones MAC	
Puerto	**Dirección MAC**
1	00-0A
4	00-0D

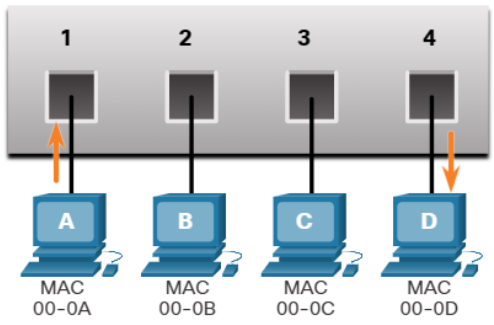


PC-A a Switch a PC-D

A continuación, PC-A envía otra trama a PC-D como se muestra en la figura. La tabla de direcciones MAC ya contiene la dirección MAC para PC-A; por lo tanto, el temporizador de actualización de cinco minutos para esa entrada se restablece. Luego, debido a que la tabla de switch contiene la dirección MAC de destino para PC-D, envía la trama solo por el puerto 4.

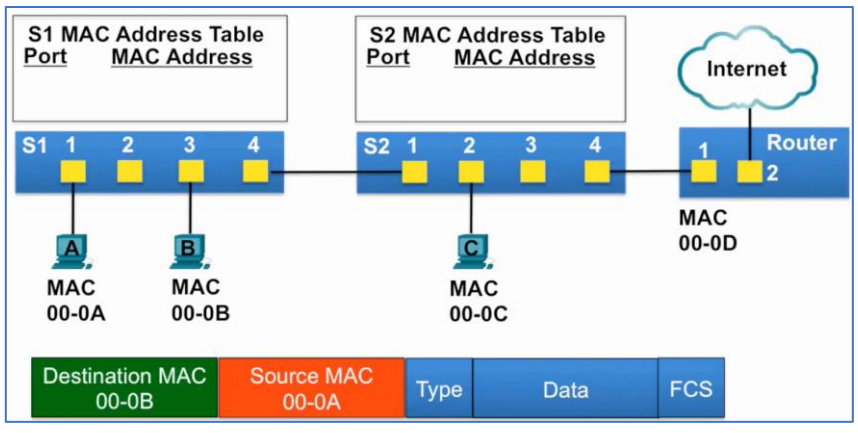
1. El switch recibe otra trama de PC-A y actualiza el temporizador para la entrada de dirección MAC del puerto 1.
2. El switch tiene una entrada reciente para la dirección MAC de destino y filtra la trama, reenviando sólo el puerto 4.

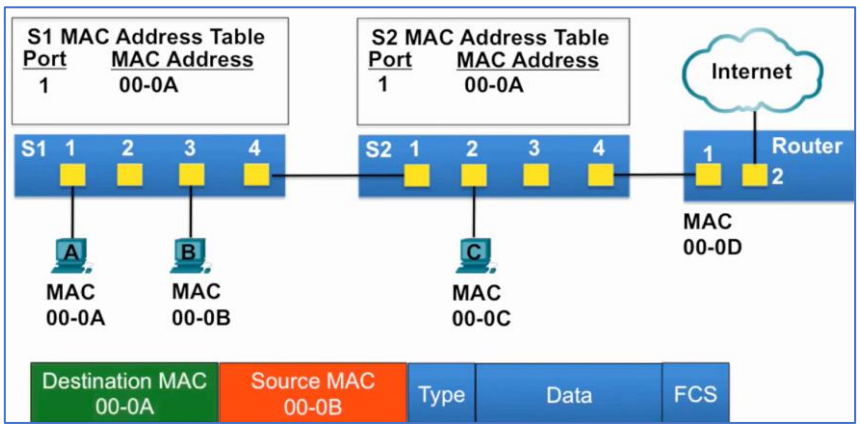
Tabla de direcciones MAC	
Puerto	**Dirección MAC**
1	00-0A
4	00-0D



4.4.4 Video - Tablas de Direcciones MAC en Conmutadores Conectados

En este video, la PCA enviará una trama de Ethernet a la PCB y la PCB enviará una trama de Ethernet a la PCA. Vamos a examinar cómo los switches S1 y S2 construyen sus tablas de direcciones Mac, y también cómo reenvían las tramas en función de la información de esas tablas de direcciones Mac. PCA tiene una trama Ethernet para enviar a PCB. La dirección Mac de origen de la trama es 000A y la dirección Mac de destino es 000B. La trama Ethernet se envía al conmutador S1, este recibe la trama Ethernet, examina la dirección Mac de origen y observa que esta dirección Mac no está en su tabla de direcciones Mac. Por lo tanto, agrega a su tabla la dirección Mac de PCA y el número de puerto entrante 1. Luego, el Switch S1 examina la dirección Mac de destino y nota que esta dirección Mac no está en su tabla, por lo que inunda todos los puertos. PCB recibe la trama Ethernet, examina la dirección Mac de destino y la compara con la suya, se da cuenta de que coincide por tanto recibe el resto de la trama. El frame Ethernet es también enviado a S2, que examina la dirección Mac de origen de la trama y nota que no está en su tabla de direcciones Mac, por tanto, S2 agrega la dirección Mac de PCA y el puerto entrante 1 a su tabla de direcciones Mac. A continuación, S2 examina la dirección Mac de destino, se da cuenta de que no está en su tabla de direcciones Mac, por lo que la inunda todos los puertos. El PCC recibe la trama de Ethernet y su dirección Mac no coincide con la dirección Mac de destino de la trama de Ethernet, por lo que no acepta el resto de la trama. El enrutador recibe la trama de Ethernet, examina la dirección Mac de destino contra la suya, no coinciden, por lo que no recibe el resto del marco. Ahora hagamos que la PCB envíe un marco de vuelta a PCA. La dirección Mac de origen del marco es 000B y la dirección Mac de destino es 000A. PCB la envía a S1 quien al darse cuenta que la dirección Mac de origen no está en su tabla de direcciones Mac, agrega la dirección Mac de PCB y el número de puerto entrante 3. A continuación, Switch S1 examina la dirección Mac de destino y nota que está en su Tabla de direcciones Mac, por lo tanto, envía la trama únicamente al puerto 1. PCA recibe la trama Ethernet, examina la dirección Mac de destino contra su propia dirección Mac y observa que coincide, por lo que recibe el resto de la trama.



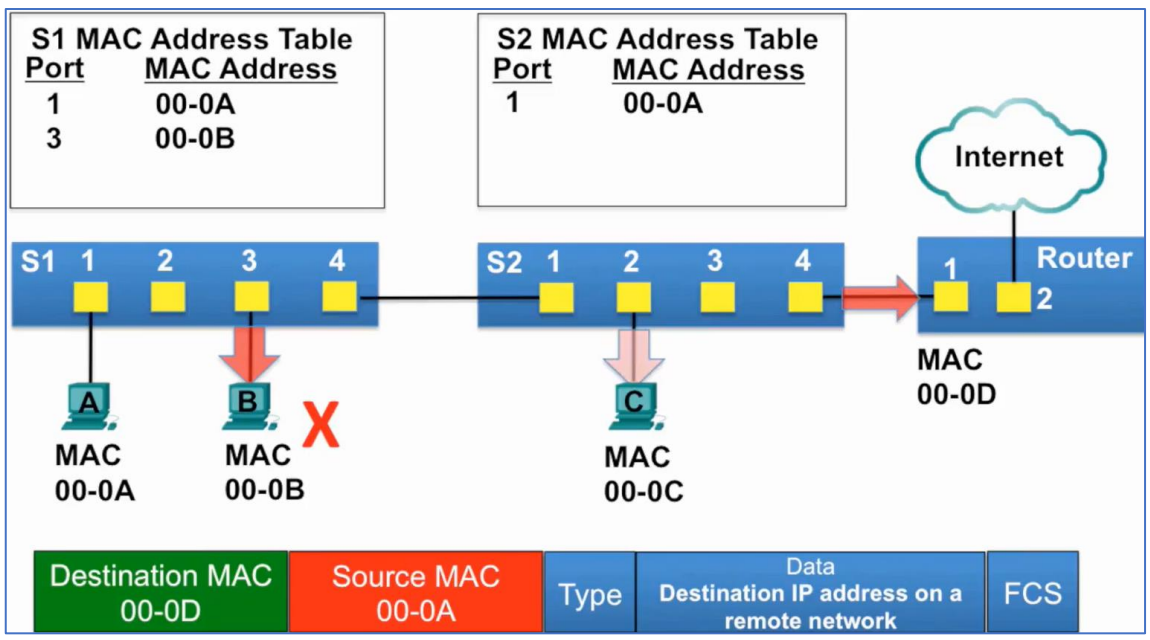


4.4.5 Video - Envío de la Trama a la Puerta de Enlace Predeterminada

Cuando un dispositivo tiene una dirección IP ubicada en una red remota, la trama de Ethernet no se puede enviar directamente al dispositivo de destino. En tal caso, la trama de Ethernet se envía a la dirección MAC del gateway predeterminado: *el router*.

Nota: En el vídeo, el paquete IP que se envía de la PC-A a un destino en una red remota, tiene como dirección IP de origen la de la PC-A y como dirección IP de destino, la del host remoto. El paquete IP de retorno tiene la dirección IP de origen del host remoto, y la dirección IP de destino es la de la PC-A.

En este video, ve que A enviará un paquete a Internet porque las direcciones IP de destino están en otra red. En este caso, la dirección Mac de origen es la de PCA, la dirección Mac de destino es la del enrutador de 000D. Entonces, la trama de Ethernet se envía al conmutador S1. El conmutador S1 recibe la trama, examina la dirección Mac de origen que se encuentra en su tabla de direcciones Mac y actualiza el temporizador de cinco minutos. Luego examina la dirección Mac de destino, comprueba que no está en su tabla de direcciones Mac, entonces inunda todos los puertos. PC-B recibe la trama Ethernet, y como la dirección Mac de destino no coincide con la suya, no acepta el resto del marco. El switch S2 reciba la trama Ethernet, examina la dirección Mac de origen, que está en su tabla de direcciones Mac, por lo que actualiza el temporizador de cinco minutos. Examina la dirección Mac de destino del marco, que no está en su tabla de direcciones Mac, por lo que la inunda todos los puertos. La PC-C obtiene la trama Ethernet, y debido a que la dirección Mac de destino no coincide con la suya, no acepta el resto de la trama Ethernet. El enrutador recibe la trama Ethernet, y debido a que la dirección Mac de destino coincide la suya, acepta el resto del marco. Ahora veremos el marco Ethernet que viene del enrutador de regreso a PCA. La dirección IP de origen es la dirección IP real de un dispositivo en una red remota. La dirección Mac de origen es la del enrutador 000D y la dirección Mac de destino es la de PCA. La trama se envía al conmutador S2, que examina la dirección Mac de origen, que no está en su tabla de direcciones Mac, por lo que la agrega. Luego examina la dirección Mac de destino, que está en su tabla de direcciones Mac, por lo que la reenvía a su Puerto # 1. S1 recibe la Ethernet marco, examina la dirección Mac de origen, que no está en su tabla de direcciones Mac, por lo que la agrega. Luego S1 examina la dirección Mac de destino, que está en su tabla de direcciones Mac, y la reenvía al Puerto # 1. PCA examina la dirección Mac de destino, y ya que es coincidente con la suya, acepta el resto del marco.



4.4.6 Actividad – Conmútelo

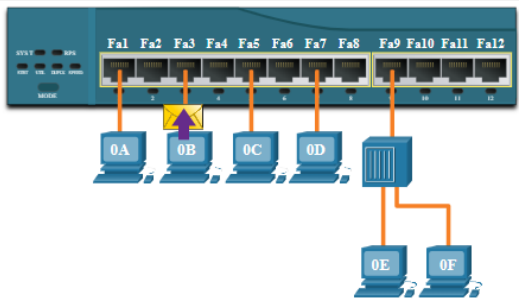
Determine cómo el conmutador reenvía una trama en función de la dirección MAC de origen, la dirección MAC de destino y la información en la tabla MAC del conmutador. Responda las preguntas utilizando la información provista.

Trama

Preámbulo	Destino MAC	Origen MAC	Tipo/Longitud	Trama	Fin de Trama
	0E	0B			

Tabla MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
		0B		0C				0E 0F			



Pregunta 1 - ¿Adónde reenviará la trama el switch?

☐Fa1 ☐Fa2 ☐Fa3 ☐Fa4 ☐Fa5 ☐Fa6 ☐Fa7 ☐Fa8 ☑Fa9 ☐FA10 ☐Fa11 ☐Fa12

Pregunta 2 - ¿Cuáles de estas afirmaciones sobre el reenvío de una trama por parte del switch son verdaderas?

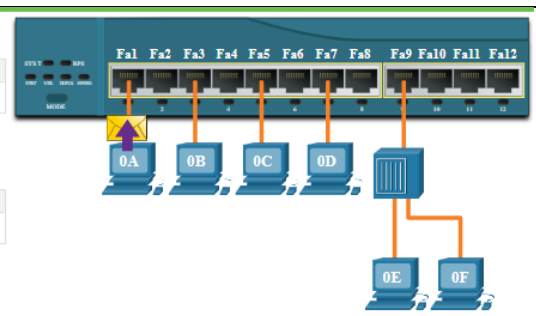
☐Switch agrega la dirección MAC de origen que actualmente no está en la tabla de direcciones MAC.
☐La trama es una trama broadcast y se reenvía a todos los puertos.
☑La trama es una trama unicast y se reenvía solamente a un puerto específico.
☐La trama es una trama unicast y se distribuye por saturación a todos los puertos.
☐La trama es unicast, pero se descarta en el switch.

Trama

Preámbulo	Destino MAC	Origen MAC	Tipo/Longitud	Trama	Fin de Trama
	0C	0A			

Tabla MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
0A		0B		0C				0F			



Pregunta 1 - ¿Adónde reenviará la trama el switch?

☐Fa1 ☐Fa2 ☐Fa3 ☐Fa4 ☑Fa5 ☐Fa6 ☐Fa7 ☐Fa8 ☐Fa9 ☐FA10 ☐Fa11 ☐Fa12

Pregunta 2 - ¿Cuáles de estas afirmaciones sobre el reenvío de una trama por parte del switch son verdaderas?

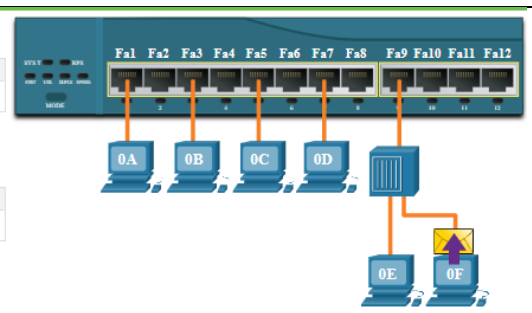
☐Switch agrega la dirección MAC de origen que actualmente no está en la tabla de direcciones MAC.
☐La trama es una trama broadcast y se reenvía a todos los puertos.
☑La trama es una trama unicast y se reenvía solamente a un puerto específico.
☐La trama es una trama unicast y se distribuye por saturación a todos los puertos.
☐La trama es unicast, pero se descarta en el switch.

Trama

Preámbulo	Destino MAC	Origen MAC	Tipo/Longitud	Trama	Fin de Trama
	0E	0F			

Tabla MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
0A		0B		0C				0F			



Pregunta 1 - ¿Adónde reenviará la trama el switch?

☑Fa1 ☐Fa2 ☑Fa3 ☐Fa4 ☑Fa5 ☐Fa6 ☑Fa7 ☐Fa8 ☐Fa9 ☐FA10 ☐Fa11 ☐Fa12

Pregunta 2 - ¿Cuáles de estas afirmaciones sobre el reenvío de una trama por parte del switch son verdaderas?

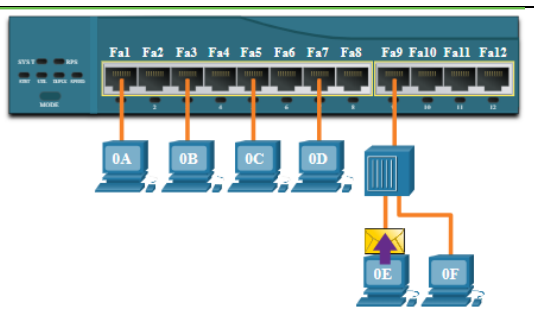
☐Switch agrega la dirección MAC de origen que actualmente no está en la tabla de direcciones MAC.
☐La trama es una trama broadcast y se reenvía a todos los puertos.
☐La trama es una trama unicast y se reenvía solamente a un puerto específico.
☑La trama es una trama unicast y se distribuye por saturación a todos los puertos.
☐La trama es unicast, pero se descarta en el switch.

Trama

Preámbulo	Destino MAC	Origen MAC	Tipo/Longitud	Trama	Fin de Trama
	0C	0E			

Tabla MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
								0E			



Pregunta 1 - ¿Adónde reenviará la trama el switch?

☑Fa1 ☐Fa2 ☑Fa3 ☐Fa4 ☑Fa5 ☐Fa6 ☑Fa7 ☐Fa8 ☐Fa9 ☐FA10 ☐Fa11 ☐Fa12

Pregunta 2 - ¿Cuáles de estas afirmaciones sobre el reenvío de una trama por parte del switch son verdaderas?

☐Switch agrega la dirección MAC de origen que actualmente no está en la tabla de direcciones MAC.
☐La trama es una trama broadcast y se reenvía a todos los puertos.
☐La trama es una trama unicast y se reenvía solamente a un puerto específico.
☑La trama es una trama unicast y se distribuye por saturación a todos los puertos.
☐La trama es unicast, pero se descarta en el switch.

5. Resumen de conmutación Ethernet

4.5.1 ¿Qué Aprendí en este Módulo?

Ethernet

No hay un protocolo oficial estándar para las redes locales, pero con el tiempo la tecnología Ethernet se volvió más habitual que las demás. Los protocolos Ethernet definen el formato de los datos y el modo como se transmiten por la red cableada. Los estándares de Ethernet especifican protocolos que funcionan en la capa 1 y en la capa 2 del modelo OSI. Ethernet se ha convertido en un estándar de facto, lo que significa que es la tecnología utilizada por casi todas las redes de área local cableadas.

El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) mantiene los estándares de red, incluidos los inalámbricos. A cada estándar de tecnología se le asigna un número que hace referencia al comité que es responsable de aprobar y mantener el estándar. El estándar 802.3 Ethernet ha mejorado con el tiempo.

Los conmutadores Ethernet pueden enviar una trama hacia todos sus puertos (excepto al puerto por el que se la recibió). Cada host que recibe esta trama examina la dirección MAC de destino y la compara con su dirección MAC. Es la tarjeta NIC Ethernet la que examina y compara la dirección MAC. Si no coincide con la dirección MAC del host, se ignora el resto de la trama. Cuando se trata de una coincidencia, ese host recibe el resto de la trama y el mensaje que contiene.

Tramas de Ethernet

Ethernet se define por los protocolos de la capa Enlace de Datos 802.2 y 802.3. Ethernet admite anchos de banda de 10 Mbps a 100 Gbps. Los protocolos IEEE 802 LAN/MAN, incluido Ethernet, usan dos subcapas separadas en la capa Enlace de Datos, LLC y MAC.

- Subcapa LLC - Esta subcapa IEEE 802.2 se comunica entre el software de red en las capas superiores y el hardware del dispositivo en las capas inferiores. Coloca en la trama información que identifica qué protocolo de capa Red se utiliza. Esta información permite que múltiples protocolos de Capa 3, como IPv4 e IPv6, utilicen la misma interfaz de red y medios.
- Subcapa MAC - Esta subcapa (IEEE 802.3, 802.11 o 802.15, por ejemplo) se implementa en hardware y es responsable de la encapsulación de datos y el control de acceso a medios. Proporciona direccionamiento de la capa Enlace de Datos y está integrada con varias tecnologías de capa Física. La encapsulación de datos incluye la trama de Ethernet, el direccionamiento de Ethernet y la detección de errores de Ethernet.

Las LAN Ethernet de hoy utilizan conmutadores que funcionan en full dúplex (completo). Las comunicaciones dúplex completo con conmutadores Ethernet no requieren control de acceso a través de CSMA/CD. El tamaño mínimo de la trama de Ethernet es de 64 bytes y el máximo esperado es de 1518 bytes. Los campos son Preámbulo y Delimitador de Inicio de Trama, Dirección MAC de Destino, Dirección MAC de Origen, Tipo/Longitud, Datos y FCS. Esto incluye todos los bytes desde el campo de dirección MAC de destino hasta el campo de secuencia de verificación de trama (FCS).

Dirección MAC de Ethernet

Una dirección MAC Ethernet consta de un valor binario de 48 bits. Se utiliza Hexadecimal para identificar una dirección Ethernet porque un solo dígito hexadecimal representa cuatro bits binarios. Por lo tanto, una dirección MAC Ethernet de 48 bits se puede expresar utilizando sólo 12 valores hexadecimales.

Una dirección MAC unicast es la dirección única que se utiliza cuando se envía una trama desde un único dispositivo de transmisión a un único dispositivo de destino. El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada con una dirección IPv4 se conoce como *Protocolo de Resolución de Direcciones (Address Resolution Protocol, ARP).* El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada con una dirección IPv6 se conoce como *Descubrimiento de Vecinos (Neighbor Discovery, ND).*

Las características de una transmisión Ethernet (broadcast) son las siguientes:

- Tiene una dirección MAC hexadecimal de destino FF-FF-FF-FF-FF-FF (48 unidades en binario).

- Se inunda hacia todos los puertos del conmutador Ethernet, excepto el puerto entrante.
- No es reenviada por un enrutador.

Las características de una multicast Ethernet (multidifusión) son las siguientes:

- Hay una dirección MAC de destino 01-00-5E cuando los datos encapsulados son un paquete de multidifusión IPv4 y una dirección MAC de destino de 33-33 cuando los datos encapsulados son un paquete de multidifusión IPv6.
- Hay otras direcciones MAC de destino de multidifusión reservadas para cuando los datos encapsulados no son IP, como STP y LLDP.
- Se inundan todos los puertos del conmutador Ethernet excepto el puerto entrante, a menos que el conmutador esté configurado para la indagación de multidifusión.
- No es reenviado por un enrutador, a menos que el enrutador esté configurado para enrutar paquetes de multidifusión.

La Tabla de direcciones MAC

Un conmutador Ethernet de capa 2 usa direcciones MAC de capa 2 para tomar decisiones de reenvío. Es completamente inconsciente de los datos (protocolo) que se transportan en la parte de datos de la trama. Un switch Ethernet examina su tabla de direcciones MAC para tomar una decisión de reenvío para cada trama. En ocasiones, la tabla de direcciones MAC se denomina tabla CAM.

El switch arma la tabla de direcciones MAC de manera dinámica después de examinar la dirección MAC de origen de las tramas recibidas en un puerto. El switch reenvía las tramas después de buscar una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC. Si la dirección MAC de destino es una dirección de unidifusión, el switch busca una coincidencia entre la dirección MAC de destino de la trama y una entrada en la tabla de direcciones MAC. Si la dirección MAC de destino está en la tabla, reenvía la trama por el puerto especificado. Si la dirección MAC de destino no está en la tabla, el switch reenvía la trama por todos los puertos, excepto el de entrada. Esto se conoce como *unicast desconocida.*

A medida que un switch recibe tramas de diferentes dispositivos, va completando su tabla de direcciones MAC examinando la dirección MAC de cada trama. Cuando la tabla de direcciones MAC del switch contiene la dirección MAC de destino, puede filtrar la trama y reenviarla a un solo puerto. Un switch puede tener muchas direcciones MAC asociadas a un solo puerto, ello cuando el switch está conectado a otro switch. El switch tiene una entrada independiente en la tabla de direcciones MAC para cada trama recibida con una dirección MAC de origen diferente. Cuando un dispositivo tiene una dirección IP ubicada en una red remota, la trama Ethernet no se puede enviar directamente al dispositivo de destino. En este caso, la trama Ethernet se envía a la dirección MAC del gateway predeterminado: el router.

4.5.2 Webster – Reflexión

Marcy y Vincent no tenían idea de cómo funcionaba su red de pequeñas empresas. No es mucho más complicado que mi propia red doméstica. No me di cuenta de que había protocolos que garantizaban la manera en que mis dispositivos interactúan entre sí y con Internet. Piense en la red de su hogar, la red en la escuela o el trabajo. ¿Entiende la diferencia entre la dirección IP de su dispositivo y su dirección MAC? ¿Cómo le ayuda este conocimiento a comprender mejor cómo funciona su red?

4.5.3 Prueba de Conmutación Ethernet

¿Qué se encapsula en el campo de datos de una trama de Ethernet?

la PDU de capa 3 ☺←	el valor de comprobación de redundancia cíclica	los bits de capa física codificados	las direcciones MAC de origen y de destino

¿Cuál es la restricción de longitud del campo de datos en una trama de Ethernet?

entre 0 y 1500 bytes	entre 46 y 1500 bytes ☺←	entre 46 y 1518 bytes	entre 46 y 1522 bytes

Consulte la ilustración. ¿Cuál es la dirección MAC de esta computadora?

```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : PC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : farfaraway.com

Ethernet adapter Local:

   Connection-specific DNS Suffix  . : farfaraway.com
   Description . . . . . . . . . . . : Ethernet Family Controller
   Physical Address. . . . . . . . . : 87-52-25-78-0F-3A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::740c:63a6:e9df:c700%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.0.24(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, September 25, 2013 09:00:08 AM
   Lease Expires . . . . . . . . . . : Monday, September 26, 2149 07:38:39 PM
   Default Gateway . . . . . . . . . : 10.0.0.1
   DHCP Server . . . . . . . . . . . : 10.0.0.1
   DHCPv6 IAID . . . . . . . . . . . : 239622969
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-15-15-BD-53-48-5B-39-A6-0F-3A
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

00-01-00-01-15-15-BD-53-48-5B-39-A6-0F-3A	87-52-25-78-0F-3A ☺←	fe80::740c:63a6:e9df:c700	fec0:0:0:ffff::1

¿Qué subcapa Ethernet se utiliza para controlar el acceso a la red mediante CSMA/CD?

LLC	MAC ☺←	enlace de datos	física

¿Qué información de direccionamiento registra un switch para armar su tabla de direcciones MAC?

la dirección de capa 3 de destino de sus paquetes entrantes	la dirección de capa 2 de destino de sus tramas salientes	la dirección de capa 3 de destino de sus paquetes salientes	la dirección de capa 2 de destino de sus tramas entrantes ☺←

¿Qué información importante examina un dispositivo de capa 2 en el encabezado de la trama de Ethernet para continuar con el reenvío de los datos?

Dirección MAC de origen	dirección IP de origen	dirección MAC de destino ☺←	Tipo de Ethernet	Dirección IP de destino

¿Qué sucede con las tramas cortas que recibe un switch Ethernet Cisco?

La trama se descarta ☺←	La trama se devuelve al dispositivo de red de origen.	La trama se transmite por broadcast a todos los demás dispositivos de la misma red.	La trama se envía al gateway predeterminado

¿Qué representa el número 100 en el estándar 100BASE-T?

Metros	Pies	Megabits por segundo ☺←	Trenzados por metro

¿Cuáles tres campos se encuentran en una trama de Ethernet 802.3? (Escoja tres opciones).

Dirección física de origen ☺←	Dirección lógica de origen	Identificador del tipo de medio
Secuencia de verificación de trama FCS ☺←	Dirección física de destino ☺←	Dirección lógica de destino

Una los componentes en la notación 100Base-T con la especificación que corresponda.

T	✓ transmisión en banda base
100	✓ cable de par trenzado
BASE	✓ velocidad en Mbps

¿Cuáles dos características describen la tecnología Ethernet? (Escoja dos).

Es compatible con los estándares IEEE 802.3 ☺←	Es compatible con los estándares IEEE 802.5.
Normalmente utiliza un promedio de 16 MB/s para velocidades de transferencia de datos	Utiliza direcciones MAC únicas para garantizar que los datos se envíen al destino adecuado. ☺←
Utiliza una topología de anillo.	

¿Qué hará un host en una red Ethernet si recibe una trama con una dirección MAC de destino de unidifusión que no coincide con su propia dirección MAC?

Se descartará la trama ☺←	Reenviará la trama al siguiente host	Eliminará la trama del medio	Se quitará la trama de enlace de datos para comprobar la dirección IP de destino.

Módulo 5: La Capa de Red

0. Introducción

5.0.1 Webster

¿Por Qué Debería Tomar este Módulo?

¡Hola de nuevo! Bob también tuvo que aprender mucho sobre la capa de red en sus cursos antes de convertirse en un especialista de TI. La capa de red, o Capa OSI 3, proporciona servicios para permitir que los dispositivos finales intercambien datos a través de redes. IPv4 e IPv6 son los principales protocolos de comunicación de la capa de red. Los protocolos de capa de red realizan cuatro operaciones: direccionamiento de dispositivos finales, encapsulación, enrutamiento y desencapsulación.

¡Suena como mucha información para personas como Marcy y Vincent que no tienen conocimientos de redes! ¿Le parece abrumador? Este módulo lo ayudará a comprender la capa de red.

5.0.2 ¿Qué Voy a Aprender en este Módulo?

Título del Módulo: La Capa de Red

Objetivo del Módulo: Explicar cómo los enrutadores usan los protocolos y servicios de la capa de red para habilitar la conectividad de un extremo a otro.

Título del Tema	Objetivo del Tema
Características de la Capa de Red	Explique la forma en que la capa de red utiliza protocolos IP para comunicaciones confiables.
Paquete IPv4	Explique la función de los principales campos de encabezado en el paquete IPv4.
Paquete IPv6	Explique la función de los principales campos de encabezado en el paquete IPv6.

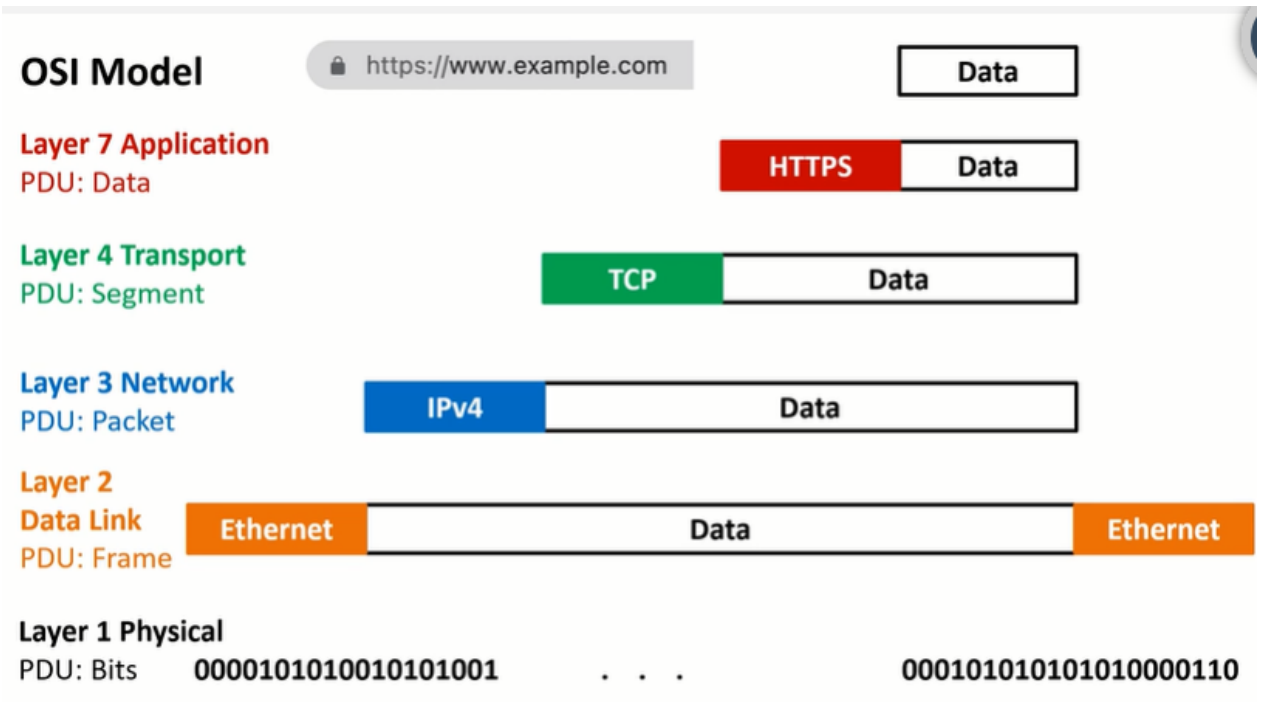
1. Características de la Capa de Red

5.1.1 Vídeo - Encapsulación de Datos

Usando el modelo OSI, echemos un vistazo a un ejemplo del proceso de encapsulación. Cuando un usuario ingresa una URL en un navegador web, esta se convierte en parte de los datos que solicitan la página del servidor web. Estos datos luego se envían al protocolo HTTPS de la Capa Aplicación en la Capa 7. El protocolo HTTPS procede encapsulando los datos con un encabezado HTTPS, aquí la PDU o unidad de datos protocolares se conoce como ***Data***. A continuación, el encabezado HTTPS y los datos originales se envían al protocolo TCP de la Capa de Transporte o Capa 4, el proceso TCP encapsula el encabezado HTTPS y los datos originales con un encabezado TCP, aquí la PDU o unidad de datos se conoce como ***Segmento***. A continuación, el Segmento TCP se envía al protocolo IPv4 de Capa de Red en la Capa 3. El protocolo IPv4 encapsula el encabezado TCP y los datos con un encabezado IPv4, aquí la PDU o unidad de datos se conoce como ***Paquete***. A continuación, el paquete IPv4 se envía al protocolo Ethernet de la Capa de Enlace de datos en la Capa 2. El protocolo Ethernet encapsula el Paquete IPv4 con una cabecera y una cola (trailer) Ethernet, aquí la PDU o unidad de datos se conoce como ***Frame***, también se le conoce como ***Trama*** o ***Marco***. Finalmente, el Frame de la Capa 2 se envía a la tarjeta de interfaz de red o NIC como bits físicos, en la Capa 1. El protocolo y los datos de cada capa se convierten en la porción de datos del siguiente protocolo. Cada protocolo acepta el encabezado del protocolo anterior en los datos y luego

encapsula esa información como datos con un encabezado de protocolo adicional. La capa de enlace de datos es la única capa que también agrega un tráiler Ethernet.

Capas OSI



5.1.2 La Capa de Red

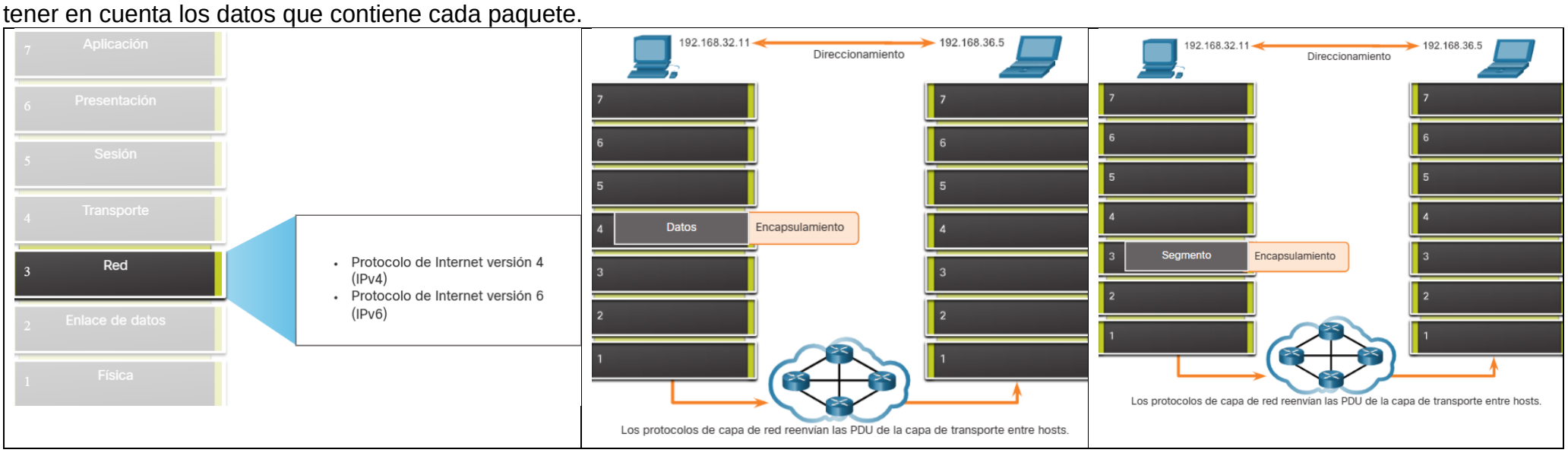
La capa de red, o Capa OSI 3, proporciona servicios para permitir que los dispositivos finales intercambien datos a través de redes. Como se muestra en la figura, IP versión 4 (IPv4) e IP versión 6 (IPv6) son los principales protocolos de comunicación de la capa de red. Otros protocolos de capa de red incluyen protocolos de enrutamiento como Open Shortest Path First (OSPF) y protocolos de mensajería como Internet Control Message Protocol (ICMP).

Protocolos de capa de red

Para lograr comunicaciones punto a punto a través de los límites de la red, los protocolos de la capa de red realizan cuatro operaciones básicas:

- **Direccionamiento de dispositivos finales** - Los dispositivos finales deben configurarse con una dirección IP única para la identificación en la red.
- **Encapsulación** - La capa de red encapsula la unidad de datos de protocolo (PDU) de la capa de transporte en un ***Paquete***. El proceso de encapsulamiento agrega información del encabezado IP, como la dirección IP de los hosts de origen (emisores) y de destino (receptores). El proceso de encapsulación lo realiza la fuente del paquete IP.
- **Enrutamiento** - La capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para transferir un paquete a otras redes, debe procesarlo un router. La función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina "enrutamiento". Un paquete puede cruzar muchos routers antes de llegar al host de destino. Se denomina "salto" a cada router que cruza un paquete antes de alcanzar el host de destino.
- **Desencapsulación** - Cuando el paquete llega a la capa de red del host de destino, el host verifica el encabezado IP del paquete. Si la dirección IP de destino dentro del encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete. Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene se transfiere al servicio apropiado en la capa de transporte. El proceso de desencapsulación lo realiza el host de destino del paquete IP.

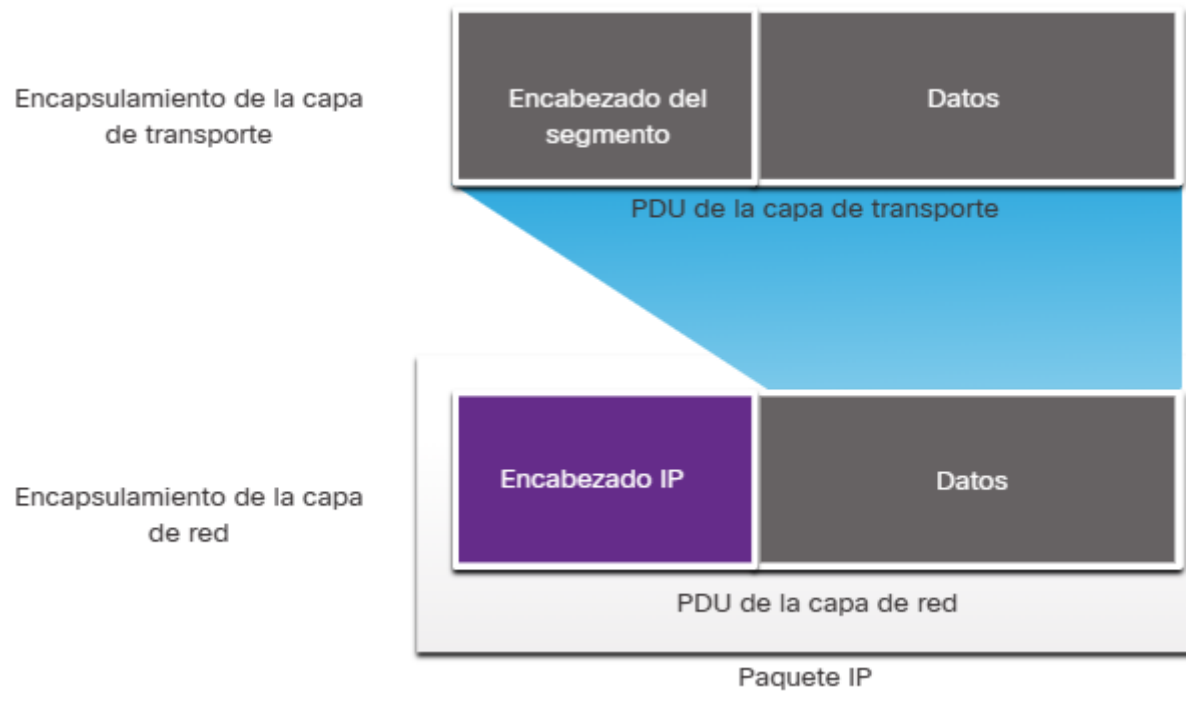
A diferencia de la Capa de Transporte (Capa OSI 4), que gestiona el transporte de datos entre los procesos que se ejecutan en cada host, los protocolos de comunicación de la Capa Red (es decir, IPv4 e IPv6) especifican la estructura de paquetes y el proceso utilizado para transportar los datos de un host a otro. La capa de red puede transportar paquetes de varios tipos de comunicación entre varios hosts porque funciona sin tener en cuenta los datos que contiene cada paquete.



5.1.3 Encapsulación IP

IP encapsula el Segmento de la Capa Transporte (la capa justo por encima de la capa de red) u otros datos agregando un encabezado IP. El encabezado IP se usa para entregar un Paquete al host de destino.

La figura ilustra cómo la PDU de la capa de transporte es encapsulada por la PDU de la capa de red para crear un paquete IP.



El proceso de encapsulamiento de datos capa por capa permite que se desarrollen y se escalen los servicios en las diferentes capas sin afectar a las otras capas. Esto significa que IPv4 o IPv6 o cualquier protocolo nuevo que se desarrolle en el futuro puede armar sin inconvenientes un paquete con los segmentos de capa de transporte.
El encabezado IP es examinado por dispositivos de Capa 3 (es decir, routers y switches de Capa 3) a medida que viaja a través de una red a su destino. Es importante tener en cuenta que la información de direccionamiento IP permanece igual desde el momento en que el paquete sale del host de origen hasta que llega al host de destino, excepto cuando se traduce por el dispositivo que realiza la traducción de direcciones de red (NAT) para IPv4.
Nota: NAT se discute en módulos posteriores.
Los routers implementan protocolos de enrutamiento para encaminar paquetes entre redes. El enrutamiento realizado por estos dispositivos intermediarios examina el direccionamiento de la capa de red en el encabezado del paquete. En todos los casos, la porción de datos del paquete, es decir, la PDU de la capa de transporte encapsulada u otros datos, permanece sin cambios durante los procesos de la capa de red.

5.1.4 Características de IP

IP se diseñó como un protocolo con sobrecarga baja. Provee solo las funciones necesarias para enviar un paquete de un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones, si es necesario, están a cargo de otros protocolos en otras capas, principalmente TCP en la capa 4.
Estas son las características básicas de IP:

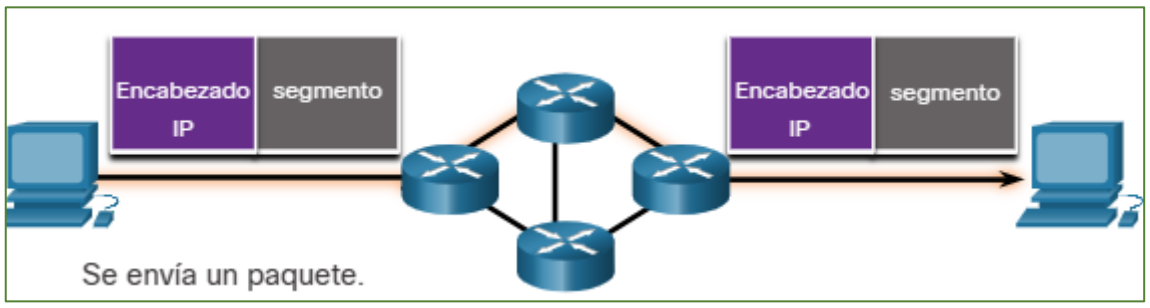
- **Sin conexión** - no hay conexión con el destino establecido antes de enviar paquetes de datos.
- **Mejor esfuerzo** - la IP es inherentemente poco confiable porque no se garantiza la entrega de paquetes.
- **Medios independientes** - la operación es independiente del medio (cobre, fibra óptica o inalámbrico) que transporta los datos.

5.1.5 Sin Conexión

IP sin conexión previa: significa que el protocolo IP no crea una conexión de extremo a extremo dedicada antes de enviar los datos. La comunicación sin conexión es como a enviar una carta a alguien sin notificar al destinatario por adelantado. La figura resume este punto clave.

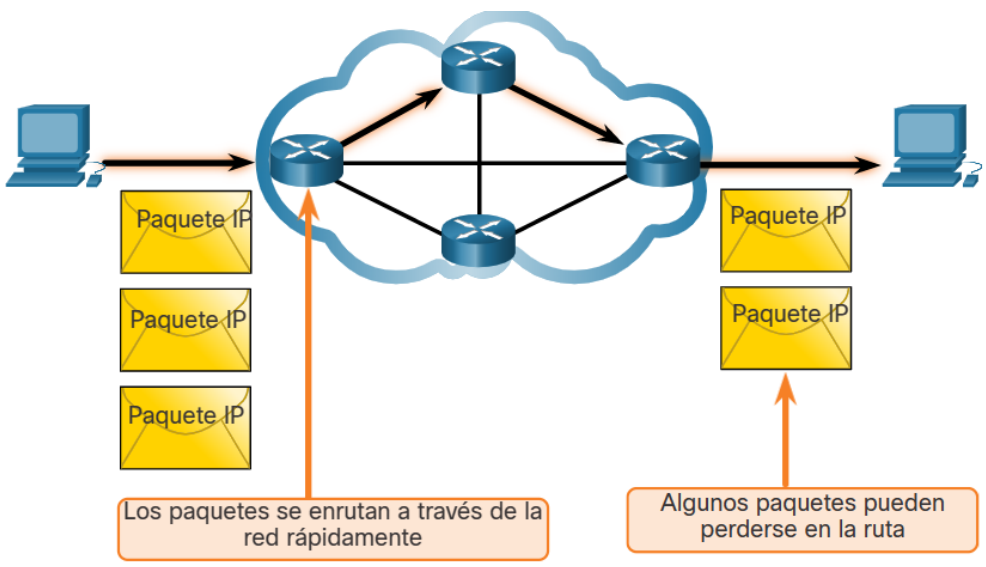
Las comunicaciones de datos sin conexión funcionan con el mismo principio. Como se muestra en la figura, el protocolo IP no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que se reenvíen los paquetes.

Sin conexión: red



5.1.6 Mejor Esfuerzo

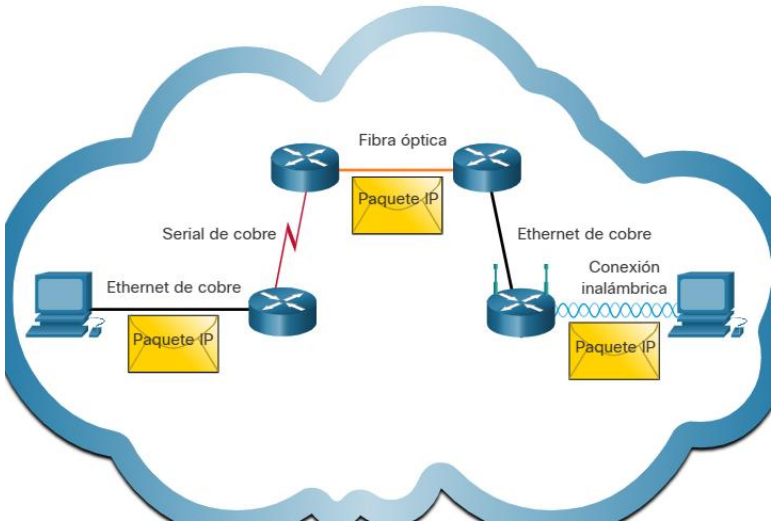
IP es un protocolo de ***mejor esfuerzo*** o ***poco confiable***: no tiene campos adicionales en el encabezado para mantener una conexión establecida.



Este proceso reduce en gran medida la sobrecarga del protocolo IP. Sin embargo, sin una conexión completa prestablecida, los remitentes no saben si los dispositivos de destino están presentes y en funcionamiento cuando envían los paquetes, ni tampoco si el destinatario recibe el paquete o si puede acceder al paquete y leerlo.
El protocolo IP no garantiza que todos los paquetes que se envían se reciban. En la ilustración, se muestran las características de entrega de mejor esfuerzo o poco confiable del protocolo IP. Dado que es un protocolo de capa de red no confiable, IP no garantiza que se reciban todos los paquetes enviados. Otros protocolos administran el proceso de seguimiento de paquetes y de aseguramiento de entrega.

5.1.7 Independiente de los Medios

Que sea poco confiable significa que el protocolo IP no tiene la capacidad para administrar y recuperar paquetes no recibidos o dañados. Esto se debe a que, si bien los paquetes IP se envían con información sobre la ubicación de la entrega, no contienen información que pueda procesarse para informar al remitente si la entrega fue exitosa. Es posible que los paquetes lleguen dañados o fuera de secuencia al destino o que no lleguen en absoluto. IP no tiene la funcionalidad de retransmitir paquetes si se producen errores.



Las aplicaciones que utilizan los datos o los servicios de capas superiores son las que deben solucionar problemas como el envío de paquetes fuera de orden o la pérdida de paquetes para permitir que el protocolo IP funcione de manera eficaz. En el conjunto de protocolos TCP/IP, la confiabilidad es la función del protocolo TCP en la capa de Transporte.

IP funciona independientemente de los medios que transportan los datos en las capas más bajas de la pila de protocolos. Como se muestra en la ilustración, los paquetes IP pueden ser señales electrónicas que se transmiten por cables de cobre, señales ópticas que se transmiten por fibra óptica o inalámbricamente por señales de radio.

Los paquetes IP pueden trasladarse a través de diferentes medios.

La capa Enlace de Datos o Capa 2 OSI es responsable de tomar un paquete IP y prepararlo para la transmisión a través del medio de comunicaciones. Esto significa que la entrega de paquetes IP no se limita a ningún medio en particular.

Sin embargo, la Capa Red tiene en cuenta una de las características más importantes del medio, que es el tamaño máximo de PDU que cada medio puede transportar. Esta característica se conoce como "unidad de transmisión máxima" (MTU). Parte del control de la comunicación entre la Capa Enlace de Datos y la Capa Red consiste en establecer el tamaño máximo del Paquete. La Capa Enlace de Datos pasa el valor de MTU a la Capa Red, esta determina qué tamaño pueden tener los Paquetes.

En algunos casos, un dispositivo intermedio, generalmente un router, debe dividir un Paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña. Este proceso se denomina ***"fragmentación de Paquetes"*** o ***"fragmentación"***. La fragmentación provoca latencia. El router no puede fragmentar los paquetes IPv6.

5.1.8 Verifique su Comprensión - Características de IP

¿Qué capa OSI envía segmentos para ser encapsulados en un paquete IPv4 o IPv6?

Capa de enlace de datos	Capa de red	Capa de transporte ☺←	Capa de sesión

*Las PDU de la capa de transporte, denominadas **segmentos**, se encapsulan en la capa de red mediante IPv4 e IPv6 en **paquetes**.*

¿Qué capa es responsable de tomar un paquete IP y prepararlo para la transmisión a través del medio de comunicación?

Capa de enlace de datos ☺←	Capa de red	Capa de transporte	Capa física

La capa de enlace de datos recibe paquetes IP de la capa de red y los encapsula para su transmisión a través del medio.

¿Cuál es el término para dividir un paquete IP al reenviarlo de un medio a otro medio con una MTU más pequeña?

Encapsulación	Fragmentación ☺←	Segmentación	Serialización

La fragmentación es el proceso de división de paquetes IP para viajar a través de un medio con una MTU más pequeña.

¿Qué método de entrega no garantiza que el paquete se entregará completamente sin errores?

Sin conexión	Mejor esfuerzo ☺←	Independiente de los medios

La entrega del mejor esfuerzo (poco confiable) no garantiza que los paquetes se entreguen al destino.

2. Paquete IPv4

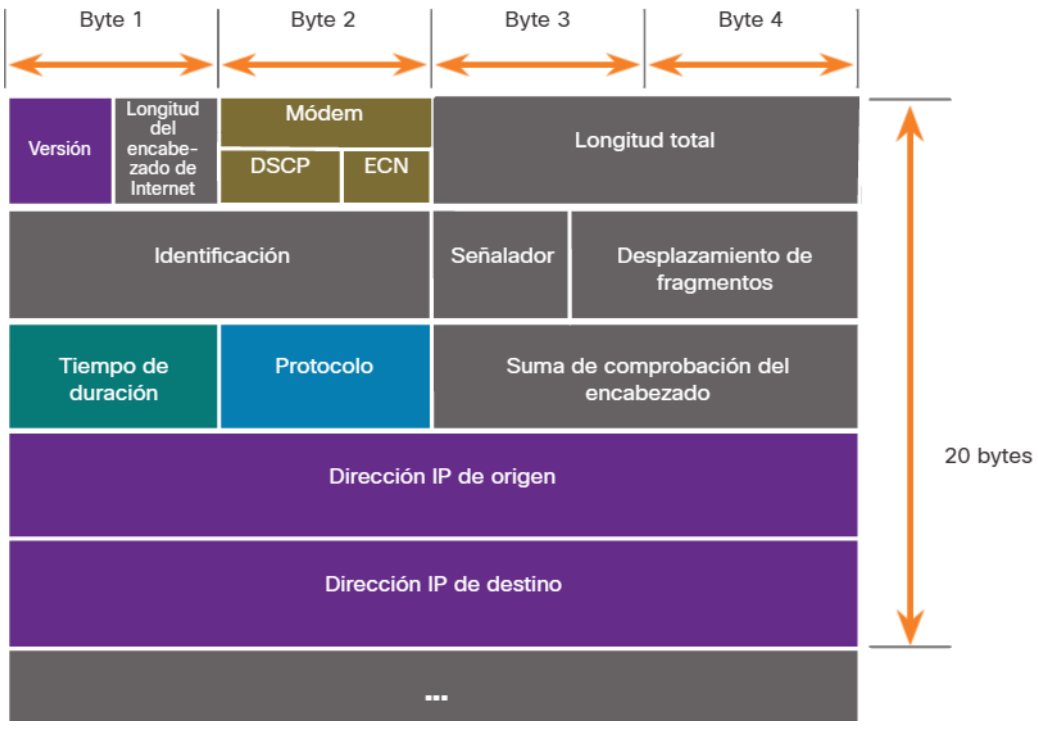
5.2.1 Encabezado del Paquete IPV4

IPv4 es uno de los principales protocolos de comunicación de la capa de red. El encabezado del paquete IPv4 se utiliza para garantizar que el paquete se entregue en su siguiente parada, en el camino a su dispositivo final de destino.

El encabezado de paquetes IPv4 consta de campos que contienen información importante sobre el paquete. Estos campos tienen números binarios que examinan el proceso de capa 3.

5.2.2 Campos del Encabezado del Paquete IPV4

Los valores binarios de cada campo identifican diversos parámetros de configuración del paquete IP. Los diagramas de encabezado del protocolo, que se leen de izquierda a derecha y de arriba hacia abajo, proporcionan una representación visual de consulta al analizar los campos de protocolo. El diagrama de encabezado del protocolo IP en la ilustración identifica los campos de un paquete IPv4.



Los campos significativos en el encabezado IPv4 incluyen lo siguiente:

- **Versión** - Contiene un valor binario de 4 bits establecido en **0100** que identifica esto como un paquete IPv4.
- **Servicios Diferenciados** o **DiffServ (DS)** - Este campo, formalmente conocido como Tipo de servicio (ToS), es un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete. Los seis bits más significativos del campo DiffServ son los bits de punto de código de servicios diferenciados (DSCP) y los dos últimos bits son los bits de notificación de congestión explícita (ECN).
- **Tiempo de Duración (Time to Live, TTL)** - El TTL contiene un valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. El dispositivo de origen del paquete IPv4 establece el valor TTL inicial. Se reduce en uno cada vez que el paquete es procesado por un router. Si el campo TTL llega a cero, el router descarta el paquete y envía a la dirección IP de origen un mensaje de tiempo superado del Protocolo de Mensajes de Control de Internet (ICMP). Debido a que el router disminuye el TTL de cada paquete, el router también debe volver a calcular la suma de comprobación del encabezado.

- **Protocolo** - Este campo se utiliza para identificar el protocolo del siguiente nivel. Este valor binario de 8 bits indica el tipo de carga de datos que lleva el paquete, lo que permite que la capa de red transmita los datos al protocolo de capa superior apropiado. ICMP (1), TCP (6) y UDP (17) son algunos valores comunes.
- **Suma de comprobación de encabezado** - Se utiliza para detectar daños en el encabezado IPv4.
- **Dirección IPv4 de origen** - Contiene un valor binario de 32 bits que representa la dirección IPv4 de origen del paquete. La dirección IPv4 de origen es siempre una dirección unicast.
- **Dirección IPv4 de destino** - Contiene un valor binario de 32 bits que representa la dirección IPv4 de destino del paquete. La dirección IPv4 de destino es una dirección unicast, multicast o de difusión.

Los dos campos a los que se hace más referencia son los de dirección IP de origen y de destino. Estos campos identifican de dónde viene el paquete y a dónde va. Por lo general, estas direcciones no cambian mientras se viaja desde el origen hasta el destino.

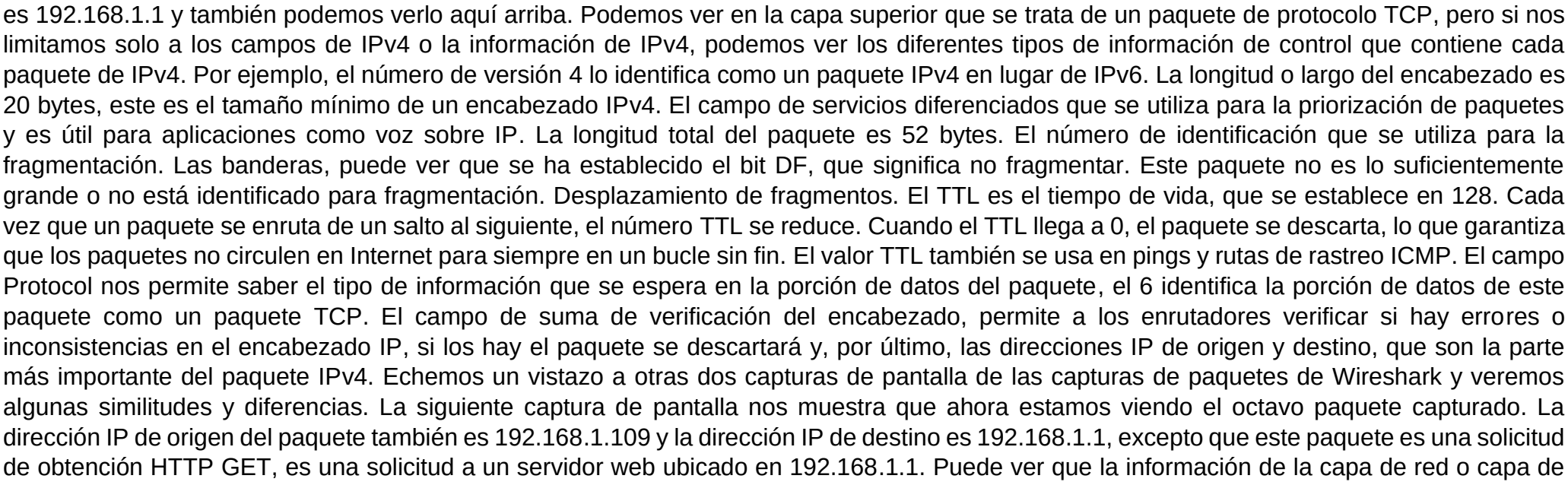
Los campos Longitud de Encabezado de Internet (IHL), Longitud Total y Suma de Comprobación del Encabezado se utilizan para identificar y validar el paquete.

Para reordenar un paquete fragmentado, se usan otros campos. Específicamente, el paquete IPv4 utiliza los campos de identificación, señaladores y desplazamiento de fragmentos para llevar un control de los fragmentos. Un router puede tener que fragmentar un paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña.

Los campos Opciones y Relleno rara vez se usan y están fuera del alcance de este módulo.

5.2.3 Video - Ejemplos del Encabezado de IPV4 en Wireshark

Tengo una captura de pantalla de mi captura de paquetes de Wireshark y puede ver que el segundo paquete que se capturó se resaltó y, luego, en la ventana de detalles del paquete, la información de la capa de red se expandió para mostrarnos todo lo que sucede en la Capa Red. Entonces, veamos qué sucede. En este paquete particular que estamos examinando, podemos ver que, en primer lugar, el protocolo de capa de red o el protocolo de capa de Internet con el que estamos tratando es el Protocolo de Internet versión 4 IPv4. También podemos ver que la dirección IP de origen era 192.168.1.109. Puede verlo también resaltado aquí en el área de la ventana de la lista de paquetes y que la dirección IP de destino es 192.168.1.1 y también podemos verlo aquí arriba. Podemos ver en la capa superior que se trata de un paquete de protocolo TCP, pero si nos limitamos solo a los campos de IPv4 o la información de IPv4, podemos ver los diferentes tipos de información de control que contiene cada paquete de IPv4. Por ejemplo, el número de versión 4 lo identifica como un paquete IPv4 en lugar de IPv6. La longitud o largo del encabezado es 20 bytes, este es el tamaño mínimo de un encabezado IPv4. El campo de servicios diferenciados que se utiliza para la priorización de paquetes y es útil para aplicaciones como voz sobre IP. La longitud total del paquete es 52 bytes. El número de identificación que se utiliza para la fragmentación. Las banderas, puede ver que se ha establecido el bit DF, que significa no fragmentar. Este paquete no es lo suficientemente grande o no está identificado para fragmentación. Desplazamiento de fragmentos. El TTL es el tiempo de vida, que se establece en 128. Cada vez que un paquete se enruta de un salto al siguiente, el número TTL se reduce. Cuando el TTL llega a 0, el paquete se descarta, lo que garantiza que los paquetes no circulen en Internet para siempre en un bucle sin fin. El valor TTL también se usa en pings y rutas de rastreo ICMP. El campo Protocol nos permite saber el tipo de información que se espera en la porción de datos del paquete, el 6 identifica la porción de datos de este paquete como un paquete TCP. El campo de suma de verificación del encabezado, permite a los enrutadores verificar si hay errores o inconsistencias en el encabezado IP, si los hay el paquete se descartará y, por último, las direcciones IP de origen y destino, que son la parte más importante del paquete IPv4. Echemos un vistazo a otras dos capturas de pantalla de las capturas de paquetes de Wireshark y veremos algunas similitudes y diferencias. La siguiente captura de pantalla nos muestra que ahora estamos viendo el octavo paquete capturado. La dirección IP de origen del paquete también es 192.168.1.109 y la dirección IP de destino es 192.168.1.1, excepto que este paquete es una solicitud de obtención HTTP GET, es una solicitud a un servidor web ubicado en 192.168.1.1. Puede ver que la información de la capa de red o capa de Internet se ha ampliado, que también es el protocolo IP versión 4, y que tenemos información similar en los diferentes campos. Observe en el campo de longitud total que este paquete tiene 411 bytes en comparación con el anterior paquete que tenía solo 52 bytes. Puede notar que este paquete tiene mucha más información, es un paquete mucho más grande que el anterior. Si miramos debajo de la información de la versión 4 del Protocolo de Internet, podemos ver la información de TCP y luego debajo de eso que también hay información sobre el protocolo de transferencia de hipertexto o el protocolo HTTP en este paquete. Pasaré al siguiente paquete, pueden ver que este paquete es la captura de paquetes número 16 aquí arriba. También es del host 192.168.1.109 al host 192.168.1.1, excepto que este es el protocolo ICMP. Puede ver la información en la ventana de la lista de paquetes que esta es una solicitud de eco o ping. En el área de detalles podemos ver algunas diferencias de menor importancia, vemos la información de la versión 4 de protocolo de Internet, la longitud del encabezado sigue siendo de 20 bytes. Pero podemos ver que las banderas son ligeramente diferentes. Y que el campo Protocolo ahora está configurado en uno, lo que indica que la porción de datos de este paquete es un mensaje de protocolo ICMP. Observe que en la ventana de detalles en la parte inferior hay un área ampliada para ver la información del encabezado específica de ICMP.



5.2.4 Verifique su Comprensión - Paquete IPv4

¿Cuáles son los dos campos a los que se hace referencia más comúnmente en un encabezado de paquete IPv4 que indican de dónde viene el paquete y hacia dónde va? (Elija dos opciones).

dirección IP de destino ☺←	protocolo	tiempo de duración	dirección IP de origen ☺←	Servicios Diferenciados (DS)

¿Qué declaración es correcta acerca de los campos de encabezado de paquetes IPv4?

Las direcciones IPv4 de origen y destino siguen siendo las mismas mientras se viaja de origen a destino. ☺←
El campo "Tiempo de vida" se utiliza para determinar la prioridad de cada paquete.
Los campos Longitud total y Suma de comprobación del encabezado se utilizan para reordenar un paquete fragmentado.
El campo Versión identifica el protocolo de siguiente nivel.

¿Qué campo se utiliza para detectar daños en el encabezado IPv4?

Suma de comprobación del encabezado ☺←	Tiempo de duración	Protocolo	Servicios diferenciados (DS)

¿Qué campo incluye valores comunes como ICMP (1), TCP (6) y UDP (17)?

Suma de comprobación del encabezado	Tiempo de duración	Protocolo ☺←	Servicios diferenciados (DS)

El campo de protocolo identifica el protocolo de capa superior que se transporta dentro del paquete IP. Los protocolos comunes son TCP, UDP e ICMP.

3. Paquete IPv6

5.3.1 Limitaciones de IPv4

IPv4 todavía está en uso hoy en día. Este tema trata sobre IPv6, que eventualmente reemplazará a IPv4. Para comprender mejor por qué necesita conocer el protocolo IPv6, debe conocer las limitaciones de IPv4 y las ventajas de IPv6.

A lo largo de los años, se han elaborado protocolos y procesos adicionales para hacer frente a los nuevos desafíos. Sin embargo, incluso con los cambios, IPv4 aún tiene tres grandes problemas:

- **Agotamiento de la dirección IPv4** - IPv4 tiene un número limitado de direcciones públicas únicas disponibles. Si bien hay aproximadamente 4000 millones de direcciones IPv4, el incremento en la cantidad de dispositivos nuevos con IP habilitado, las conexiones constantes y el crecimiento potencial de regiones menos desarrolladas aumentaron la necesidad de direcciones.
- **Falta de conectividad de extremo a extremo** - La traducción de direcciones de red (NAT) es una tecnología comúnmente implementada dentro de las redes IPv4. NAT proporciona una manera para que varios dispositivos compartan una única dirección IPv4 pública. Sin embargo, dado que la dirección IPv4 pública se comparte, se oculta la dirección IPv4 de un host de la red interna. Esto puede ser un problema para las tecnologías que necesitan conectividad completa.
- **Mayor complejidad de la red** - Mientras que NAT ha ampliado la vida útil de IPv4, solo se trataba de un mecanismo de transición a IPv6. NAT en sus diversas implementaciones crea una complejidad adicional en la red, creando latencia y haciendo más difícil la solución de problemas.

5.3.2 Descripción General de IPv6

A principios de la década de 1990, los problemas con IPv4 preocuparon al Grupo de Trabajo de Ingeniería de Internet (IETF) que, en consecuencia, comenzó a buscar un reemplazo. Esto tuvo como resultado el desarrollo de IP versión 6 (IPv6). IPv6 supera las limitaciones de IPv4 y representa una mejora importante con características que se adaptan mejor a las demandas de red actuales y previsibles.

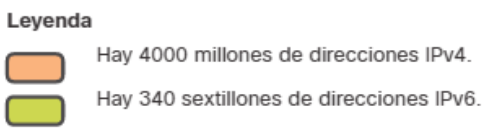
Las mejoras que ofrece IPv6 incluyen las siguientes:

- **Mayor Espacio de Direcciones** - Las direcciones IPv6 se basan en direcciones jerárquicas de 128 bits en lugar de IPv4 con 32 bits.
- **Manejo de Paquetes Mejorado** - El encabezado de IPv6 se ha simplificado con menos campos.
- **Elimina la necesidad de NAT** - Con una cantidad tan grande de direcciones IPv6 públicas, no se necesita NAT entre una dirección IPv4 privada y una IPv4 pública. Esto evita algunos de los problemas inducidos por NAT que experimentan las aplicaciones que requieren conectividad de extremo a extremo.

El espacio de las direcciones IPv4 de 32 bits ofrece aproximadamente 4,294'967,296 direcciones IP únicas. El espacio de direcciones IPv6 proporciona $340^{6}282{,}366^{5}920{,}938^{4}463{,}463^{3}374{,}607^{2}431{,}768'211{,}456$ o 340 sextillones de direcciones. Esto es aproximadamente equivalente a cada grano de arena en la Tierra.

En la ilustración, se puede ver una comparación entre el espacio de direcciones IPv4 e IPv6.

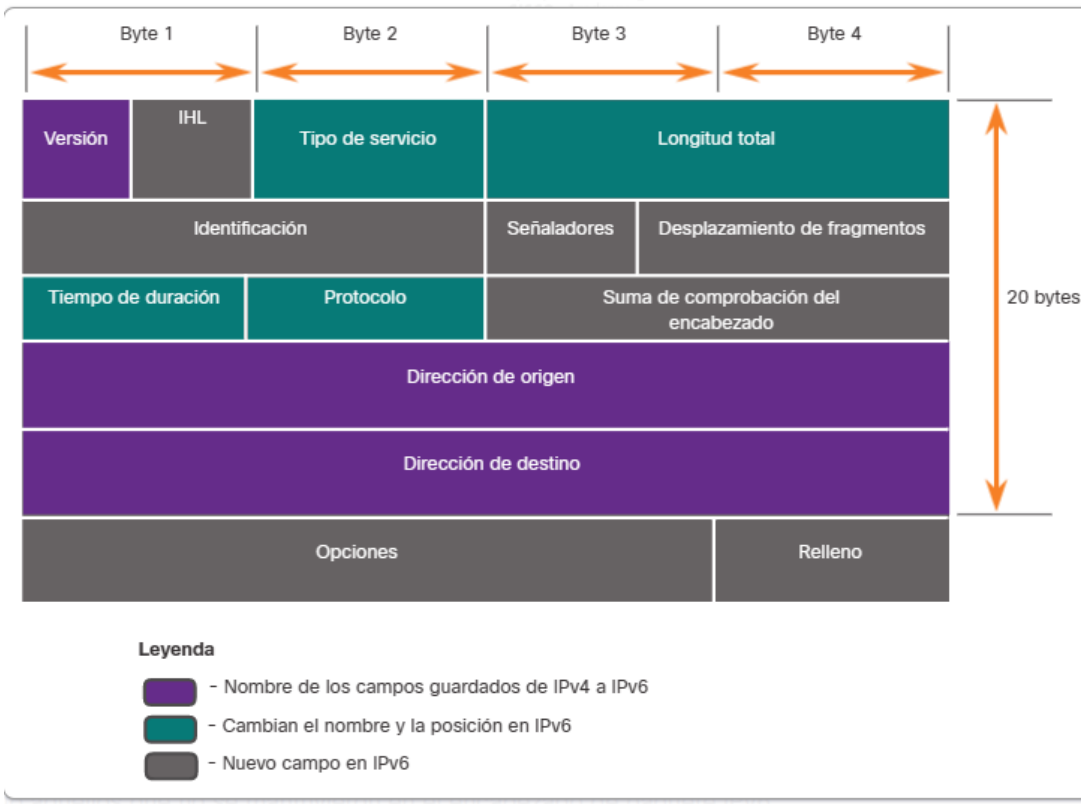
Nombre del número	Notación científica	Cantidad de ceros
Mil	10^3	1000
1 millón	10^6	1 000000
1000 millones	10^9	1000000000
1 billón	10^12	1000000000000
1000 billones	10^15	1000000000000000
1 trillón	10^18	1000000000000000000
1000 trillones	10^21	1000000000000000000000
1 cuatrillón	10^24	1000000000000000000000000
1000 cuatrillones	10^27	1000000000000000000000000000
1 quintillón	10^30	1000000000000000000000000000000
1000 quintillones	10^33	1000000000000000000000000000000000
1 sextillón	10^36	1000000000000000000000000000000000000



5.3.3 Campos del Encabezado del Paquete IPv4 en el Encabezado del Paquete IPv6

Uno de las mejoras de diseño más importantes de IPv6 con respecto a IPv4 es el encabezado simplificado de IPv6.

Encabezado del Paquete IPv4

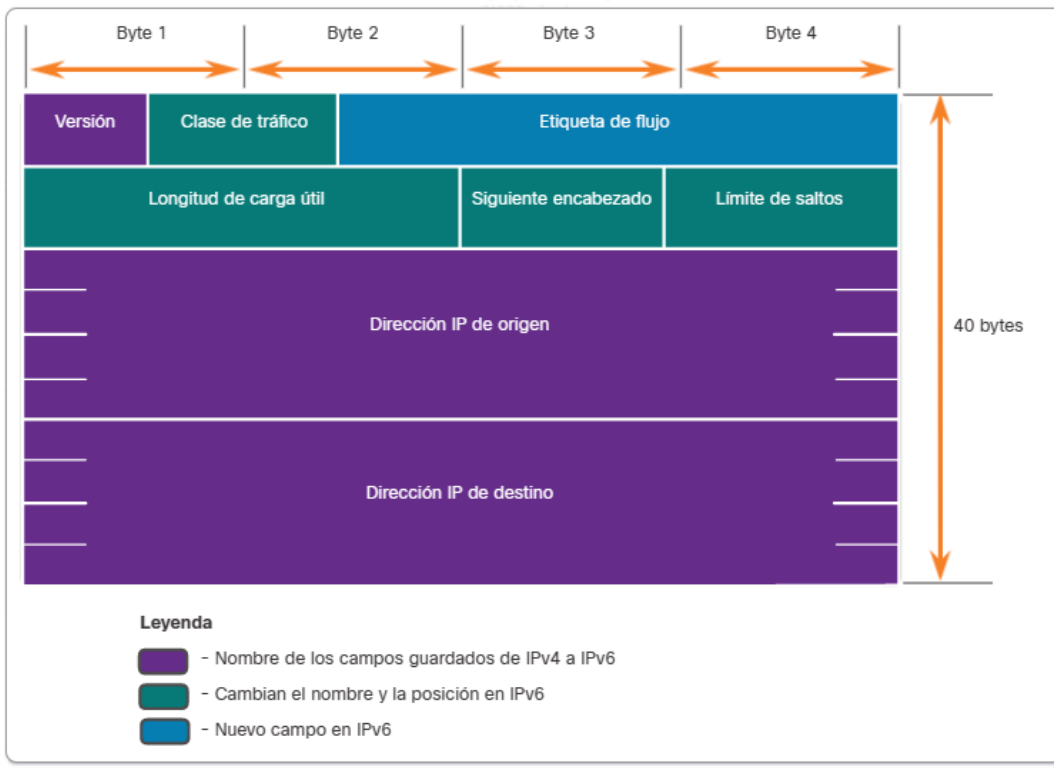


Por ejemplo, el encabezado IPv4 consiste en un encabezado de longitud variable de 20 octetos (hasta 60 bytes si se usa el campo Opciones) y 12 campos de encabezado básicos, sin incluir el campo Opciones y el campo Relleno.

Para IPv6, algunos campos se han mantenido igual, algunos campos han cambiado de nombre y posición, y algunos campos de IPv4 ya no son necesarios, como se destaca en la figura.

La figura muestra los campos de encabezado de paquete IPv4 que se mantuvieron, movieron, cambiaron, así como aquellos que no se mantuvieron en el encabezado de paquete IPv6.

Encabezado del Paquete IPv6



El encabezado simplificado IPv6 permite un procesamiento más eficiente, consiste en un encabezado de longitud fija de 40 octetos (en gran parte debido a la longitud de las direcciones IPv6 de origen y destino).

5.3.4 Encabezado del Paquete IPv6

Los campos en el encabezado del paquete IPv6 incluyen lo siguiente:

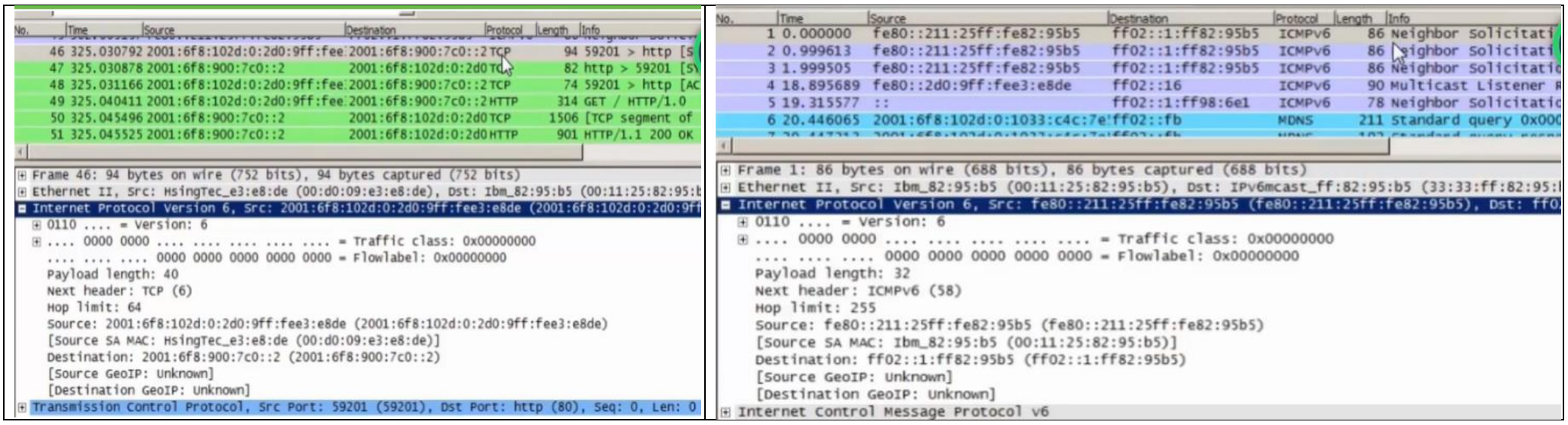
- **Versión -** Este campo contiene un valor binario de 4 bits establecido en 0110 que identifica esto como un paquete IP versión 6.
- **Clase de Tráfico -** Este campo de 8 bits es el equivalente al campo Servicios Diferenciados (DS) de IPv4.
- **Etiqueta de Flujo -** Este campo de 20 bits sugiere que todos los routers manipulen del mismo modo los paquetes con la misma etiqueta de flujo.
- **Longitud de Carga Útil -** Este campo de 16 bits indica la longitud de la parte de los datos o la carga útil del paquete IPv6. Esto no incluye la longitud del encabezado IPv6, que es un encabezado fijo de 40 bytes.
- **Siguiente Encabezado -** Este campo de 8 bits equivale al campo Protocolo IPv4. Es un valor que indica el tipo de contenido de datos que lleva el paquete, lo que permite que la capa de red transmita la información al protocolo de capa superior apropiado.
- **Límite de Saltos -** Este campo de 8 bits reemplaza al campo TTL de IPv4. Cada router que reenvía el paquete reduce este valor en 1. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje ICMPv6 Tiempo excedido al host emisor. Esto indica que el paquete no llegó a su destino porque se excedió el límite de saltos. A diferencia de IPv4, IPv6 no incluye una suma de comprobación de encabezado IPv6, ya que esta función se realiza tanto en las capas inferior como superior. Esto significa que la suma de comprobación no necesita ser recalculada por cada router cuando disminuye el campo Límite de saltos, lo que también mejora el rendimiento de la red.
- **Dirección IPv6 de Origen -** Este campo de 128 bits identifica la dirección IPv6 del host emisor.
- **Dirección IPv6 de Destino -** Este campo de 128 bits identifica la dirección IPv6 del host receptor.

Un paquete IPv6 también puede contener encabezados de extensión (EH), que proveen información optativa de la capa de red. Los encabezados de extensión son opcionales y están ubicados entre el encabezado de IPv6 y el contenido. Los EH se usan para fragmentar, dar seguridad, admitir la movilidad y otras acciones.
A diferencia de IPv4, los routers no fragmentan los paquetes IPv6 enrutados.

5.3.5 Video - Ejemplos del Encabezado IPV6 en Wireshark

Esta captura de pantalla muestra una captura de paquetes usando Wireshark y la información de la capa de red de una conversación IPv6. Echémosle un vistazo. En esta captura de pantalla podemos ver que el paquete resaltado es el paquete #46. Y que la dirección de origen aquí arriba en la ventana de la lista de paquetes muestra que es una dirección IPv6 de unidifusión global. Puede ver que esto comienza con 2001:6f8. La dirección de destino también es una dirección de unidifusión global 200:6f8:900 y así sucesivamente. Y si observamos el campo de protocolo, vemos que en las capas superiores se trata de un paquete TCP que intenta establecer una comunicación inicial con un servidor web HTTP. Si miramos hacia abajo en el área de información de la capa de red, puede ver que la información de IPv6 se ha ampliado. Echemos un vistazo a parte de la información del campo de protocolo para el Protocolo de Internet versión 6. En primer lugar, puede ver que la cantidad de información

en el encabezado IPv6 es mucho menor que en el encabezado IPv4. Ahora hay algunas características interesantes. Por un lado, puede ver que el campo Versión en este caso dice 6, identificando este paquete como IPv6. También podemos ver el 6 binario aquí. El siguiente campo es el campo de clase de tráfico. El campo de clase de tráfico cumple la misma función que el campo de servicios diferenciados en un paquete IPv4, maneja la priorización del tráfico y la congestión. La siguiente sección que puede ver es la etiqueta de flujo. El campo de etiqueta de flujo es un campo nuevo para el protocolo IPv6. Su propósito es mantener los mismos flujos de paquetes a través de enrutadores y conmutadores para ayudar a las aplicaciones en tiempo real que necesitan que los paquetes lleguen en el mismo orden. Podría ver que el siguiente campo es el campo de longitud de la carga útil. Esto es lo mismo que el campo de longitud total en el encabezado IPv4. Este campo nos dice el tamaño total del paquete, en este caso 40 bytes. El siguiente campo de encabezado tiene el mismo propósito que el campo de protocolo para IPv4. Puede ver que identifica que la porción de datos de la capa superior de este paquete es 6 o TCP. El límite de salto cumple la misma función que el campo TTL en un paquete IPv4. Puede ver que el límite de saltos actualmente está establecido en 64 saltos. Una vez que esto disminuya a cero, el paquete se descartará. A continuación, tenemos la dirección IPv6 de origen, la dirección IPv6 de destino y luego, en la capa superior, podemos ver que este es un paquete TCP con información de encabezado TCP. Echemos un vistazo a la siguiente captura de pantalla. En la siguiente captura de pantalla, puede ver que ahora hemos resaltado el paquete n.º 49 y ahora tenemos una conexión con este servidor web. Este paquete ahora es una solicitud de obtención al servidor web. Si miramos hacia abajo en el paquete ampliado de la versión seis del Protocolo de Internet, en la ventana de detalles, podemos ver que la longitud de la carga útil es mucho mayor, y que ahora también hay información del protocolo HTTP dentro de nuestra solicitud de obtención. Esta es nuestra solicitud de obtención para obtener una página web. Si voy a la siguiente captura de pantalla, la última captura de pantalla muestra un mensaje de solicitud de vecino ICMP versión 6. Si buscamos en la ventana el paquete resaltado aquí y el paquete número uno, veremos que la dirección de origen esta vez no es una dirección IPv6 de unidifusión global, sino una dirección local de enlace. Podemos decir eso por el fe80 aquí. También podemos ver que esta dirección local de enlace usó EUI 64 para resolver la parte de identificación de interfaz de la dirección. Podemos decir eso por la ff:fe dentro de la dirección. La dirección de destino es una dirección FF02 IPv6, lo que indica que se trata de un paquete de multidifusión. Si revisamos el protocolo, vemos que es ICMP versión 6 y luego la información sobre el paquete nos dice que este es un mensaje de solicitud de vecino para el mismo dispositivo que contactamos en las capturas de pantalla anteriores. La función de este paquete es esencialmente similar a una búsqueda ARP en IPv4. Necesitamos descubrir la dirección local del enlace de este dispositivo, por lo que enviamos un mensaje de solicitud de vecino ICMP versión 6, devuelve una dirección local de enlace de este vecino. Si miramos hacia abajo en la ventana de detalles ampliada, podemos ver que la versión tiene una longitud de carga útil de etiqueta de flujo de clase de tráfico 6, que es la longitud total del paquete. El siguiente campo de encabezado, que es como el campo de protocolo en IPv4, indica 58, por lo que este es un mensaje ICMP versión 6 en la parte de datos del paquete. El límite de saltos es de 255 saltos. Esto es similar al campo TTL. Luego la dirección local del enlace de origen y la dirección IPv6 de multidifusión de destino en la parte inferior. Debajo de la información de IPv6 podemos ver que hay un área expandible específica al protocolo de mensajes de control de Internet versión 6.



5.3.6 Verifique su Comprensión - Paquete IPv6

¿Cuáles son las tres opciones principales problemas asociados con IPv4? (Elija tres opciones).

- Agotamiento de direcciones IP ☺←
- Mayor complejidad de la red y expansión de la tabla de enrutamiento de Internet ☺←
- Siempre en conexiones
- Falta de conectividad de extremo a extremo ☺←
- Fronteras mundiales y políticas
- Demasiadas direcciones IPv4 disponibles

IPv4 se estandarizó en la década de 1980 y tiene varias limitaciones tecnológicas, como la falta de conectividad de extremo a extremo y un espacio de direcciones agotado.

¿Cuáles dos opciones son mejoras proporcionadas por IPv6 en comparación con IPv4? (Elija dos opciones).

- Admite campos adicionales para paquetes complejos
- Aumentó el espacio de la dirección IP ☺←
- Estandariza el uso de NAT
- Admite redes basadas en clases
- Utiliza un encabezado más simple para proporcionar un manejo mejorado de paquetes ☺←

Hay varias mejoras técnicas realizadas en IPv6, dos de las cuales son un grupo de direcciones IP mucho más grande y un encabezado de protocolo simplificado.

¿Qué es verdadero para el encabezado IPv6? (Elija dos opciones).

- Consta de 20 octetos.
- Consta de 40 octetos. ☺←
- Contiene 8 campos de encabezado. ☺←
- Contiene 12 campos de encabezado.

El encabezado IPv6 tiene una longitud fija de 40 octetos y contiene 8 campos de encabezado.

¿Cuál es el verdadero del encabezado del paquete IPv6?

- El campo Límite de salto reemplaza el campo Tiempo de vida IPv4. ☺←
- Las direcciones IPv6 de origen y destino cambian mientras se viaja de origen a destino.

El campo Tiempo de vida reemplaza al campo DiffServ.
El campo Versión identifica el siguiente encabezado.

Varios campos del encabezado IPv6 reemplazaron los campos del encabezado IPv4. Por ejemplo, el campo Límite de saltos reemplazó al campo Tiempo de vida del encabezado IPv4.

4. Resumen de la Capa de Red

5.4.1 ¿Qué Aprendí en este Módulo?

Características de la Capa Red

La capa de red, o Capa OSI 3, proporciona servicios para permitir que los dispositivos finales intercambien datos a través de redes. IPv4 e IPv6 son los principales protocolos de comunicación de la capa de red. Otros protocolos de capa de red incluyen protocolos de enrutamiento como OSPF y protocolos de mensajería como ICMP.

Los protocolos de capa de red realizan cuatro operaciones: direccionamiento de dispositivos finales, encapsulación, enrutamiento y desencapsulación. IPv4 e IPv6 especifican la estructura de paquetes y el procesamiento utilizado para transportar los datos de un host a otro. La capa de red puede transportar paquetes de varios tipos de comunicación entre varios hosts porque funciona sin tener en cuenta los datos que contiene cada paquete.

Para encapsular el segmento de capa de transporte u otros datos, le agrega un encabezado IP. El encabezado IP se usa para entregar el paquete al host de destino. El encabezado IP es examinado por enrutadores y conmutadores de capa 3 a medida que viaja a través de una red hasta su destino. La información de direccionamiento IP permanece igual desde el momento en que el paquete sale del host de origen hasta que llega al host de destino, excepto cuando la traduce el dispositivo que realiza NAT para IPv4.

Las características de la IP son que es: sin conexión, mejor esfuerzo (poco confiable) e independiente de los medios de comunicación. IP sin conexión, significa que el protocolo IP no crea una conexión de extremo a extremo dedicada antes de enviar los datos. IP no necesita campos adicionales en el encabezado para mantener una conexión establecida. Este proceso reduce la sobrecarga del protocolo IP. Los remitentes no saben si los dispositivos de destino están presentes y en funcionamiento cuando envían paquetes, ni tampoco si el destinatario recibe el paquete o si puede acceder al paquete y leerlo. IP funciona independientemente de los medios que transportan los datos en las capas más bajas de la pila de protocolos. Los paquetes IP pueden ser comunicados por medio de señales electrónicas que se transmiten por cables de cobre, señales ópticas que se transmiten por fibra óptica o señales de radio inalámbricas. Una característica de los medios que considera la capa de red es el tamaño máximo de la PDU que cada medio puede transportar, o la MTU.

Paquete IPv4

El encabezado del paquete IPv4 se utiliza para garantizar que un paquete se entrega a su siguiente parada en el camino a su dispositivo final de destino. Un encabezado de paquete IPv4 consiste en campos que contienen números binarios que son examinados por el proceso de Capa 3. Los campos significativos en el encabezado de IPv4 incluyen: versión, DS, TTL, protocolo, suma de verificación del encabezado, dirección IPv4 de origen y dirección IPv4 de destino.

Los campos Longitud de Encabezado de Internet (IHL), Longitud Total y Suma de Comprobación del Encabezado se utilizan para identificar y validar el paquete. El paquete IPv4 utiliza los campos de Identificación, Señaladores y Desplazamiento de Fragmentos para llevar un control de los fragmentos. Un router puede tener que fragmentar un paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña.

Paquete IPv6

IPv4 tiene limitaciones, que incluyen: agotamiento de direcciones IPv4, falta de conectividad de extremo a extremo y una mayor complejidad de la red. IPv6 vence las limitaciones de IPv4. Las mejoras que ofrece IPv6 incluyen lo siguiente: mayor espacio de direcciones, mejor manejo de paquetes y elimina la necesidad de NAT.

El espacio de las direcciones IPv4 de 32 bits ofrece aproximadamente 4.294.967.296 direcciones únicas. El espacio de direcciones IPv6 proporciona 340,282,366,920,938,463,463,374,607,431,768,211,456, o 340 sextillones (undecillones) de direcciones. Esto es aproximadamente equivalente a cada grano de arena en la Tierra.

Los campos de encabezado simplificados de IPv6 incluyen: versión, clase de tráfico, etiqueta de flujo, longitud de carga útil, siguiente encabezado, límite de salto, dirección IP de origen y dirección IP de destino. Un paquete IPv6 también puede contener Encabezados de Extensión (EH), que proveen información opcional de la capa de red. Los encabezados de extensión son opcionales y están ubicados entre el encabezado de IPv6 y el contenido. Los EH se usan para fragmentar, dar seguridad, admitir la movilidad y otras acciones. A diferencia de IPv4, los routers no fragmentan de los paquetes IPv6 enrutados.

5.4.2 Webster - Preguntas de Reflexión

¡Más protocolos! Estoy empezando a comprender que se realizó una gran cantidad de trabajo para crear estos protocolos. En la capa de red, los protocolos se encargan del direccionamiento, de la encapsulación de los datos, del enrutamiento de los paquetes y de la desencapsulación de los paquetes para que puedan leerse. Marcy y Vincent no son profesionales de TI, por lo que una red en funcionamiento puede parecerles un poco misteriosa. Pero ayuda saber qué sucede en la capa de red del modelo OSI. ¿Cómo puede este conocimiento ayudarlo a solucionar problemas de su propia red?

5.4.3 Prueba de la Capa de Red

¿Qué valor, contenido en un campo de encabezado IPv4, disminuye cada enrutador que recibe un paquete?

Servicios diferenciados	Desplazamiento de fragmentos	Longitud del encabezado	Tiempo de duración ☺←

¿Qué enunciado describe con precisión una característica de IPv4?

Todas las direcciones IPv4 se pueden asignar a hosts.
IPv4 tiene un espacio de direcciones de 32 bits. ☺←
Un encabezado IPv4 tiene menos campos que un encabezado IPv6.
IPv4 admite de forma nativa IPSec.

¿Qué tecnología proporciona una solución para el agotamiento de la dirección IPv4 al permitir que varios dispositivos compartan una dirección IP pública?

ARP	DNS	NAT ☺←	SMB	DHCP	HTTP

¿Por qué IPv6 está diseñado para reemplazar a IPv4?

- porque la mayoría de las computadoras tienen un procesador de 64 bits
- porque el espacio de direcciones IPv4 se agotará pronto ☺←
- para permitir que las computadoras direccionen más memoria
- para abordar problemas de compatibilidad con dispositivos móviles

¿Qué característica de la capa de red del modelo OSI permite transportar paquetes para varios tipos de comunicación entre muchos hosts?

- El desencapsulamiento de los encabezados provenientes de capas inferiores
- La selección de rutas para el destino y los paquetes directos hacia él
- La capacidad de operar independientemente de los datos que se transportan en cada paquete ☺←
- La capacidad de administrar el transporte de datos entre los procesos que se ejecutan en los hosts

¿Qué enunciado describe una característica de la capa de red en el modelo OSI?

- Gestiona el transporte de datos entre los procesos que se ejecutan en cada host.
- En el proceso de encapsulación, agrega números de puerto de origen y destino al encabezado IP.
- Cuando un paquete llega al host de destino, la capa de red verifica su encabezado IP para determinar hacia dónde debe enrutarse el paquete. ☺←
- Sus protocolos especifican la estructura del paquete y el procesamiento utilizado para transportar los datos de un host a otro.

¿Cuál capa del modelo OSI es responsable del direccionamiento lógico de los paquetes?

Enlace de datos	Red ☺←	Sesión	Transporte

¿Cuál es el orden de encapsulación para las unidades de datos de protocolo que pasan de la aplicación del usuario hacia abajo en la pila?

- bits, segmentos, paquetes, tramas, datos
- datos, segmentos, paquetes, tramas, bits ☺←
- segmentos, datos, paquetes, tramas, bits
- segmentos, paquetes, tramas, bits, datos

¿Qué proceso implica colocar una PDU dentro de otra PDU?

Encapsulación ☺←	Codificación	Segmentación	Control de Flujo

¿Qué información se agrega durante el encapsulamiento en la capa 3 del modelo OSI?

- Dirección MAC de origen y destino
- Protocolo de aplicaciones de origen y destino
- Número de puertos de origen y destino
- Dirección IP de origen y destino ☺←

¿Cómo utiliza la capa de red el valor de MTU?

- La capa de red depende de las capas de niveles superiores para determinar la MTU.
- La capa de red depende de la capa de enlace de datos para establecer la MTU y ajusta la velocidad de transmisión para admitirla.
- La capa de enlace de datos pasa la MTU a la capa de red. ☺←
- Para aumentar la velocidad de entrega, la capa de red ignora la MTU.

Módulo 6: Direccionamiento IPv4

0. Introducción

6.0.1 Webster - ¿Por qué debería tomar este módulo?

Bob ha investigado la red actual y les ha asegurado a Marcy y Vincent que pueden usarla hasta que realice las actualizaciones. Bob ha convencido a Marcy y Vincent para crear una nueva red jerárquica que utilizará servicios en la nube. Con la investigación y las explicaciones de las redes de Bob, están seguros de que esta es la mejor opción para ellos. ¡Realmente aprecian el conocimiento de Bob!

Quizás tenga un largo camino por recorrer antes de tener todos los conocimientos y habilidades de Bob, pero creo que está en el camino correcto. Este módulo profundizará en el direccionamiento IPv4. ¿Está listo? Continúe leyendo.

6.0.2 ¿Qué Voy a Aprender en este Módulo?

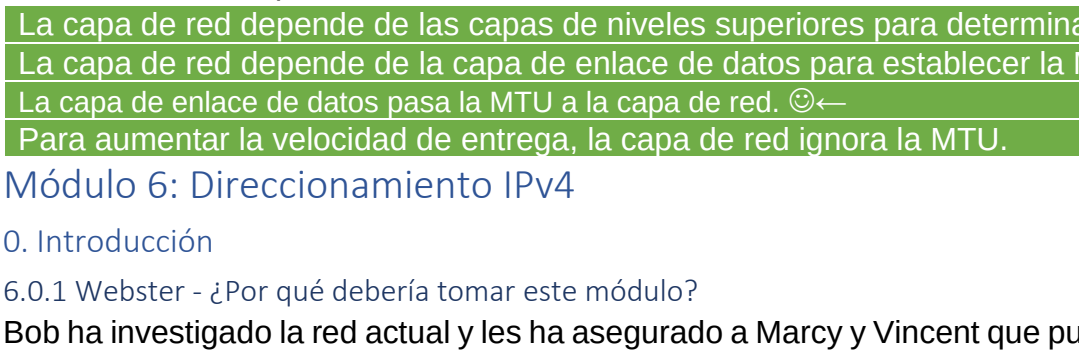
- Título del Módulo: Direccionamiento IPv4
- Objetivo del Módulo: Calcular un esquema de división en subredes IPv4 para segmentar una red de manera eficiente.

Título del Tema	Objetivo del Tema
Estructura de Direcciones IPv4	Describa la estructura de una dirección IPv4, incluidas la porción de red y de host, y la máscara de subred.

1. Estructura de la dirección IPv4

6.1.1 Porciones de Red y de Host

Una dirección IPv4 es una dirección jerárquica de 32 bits que se compone de una porción de red y una porción de host. Al determinar la porción de red frente a la porción del host, debe mirar la secuencia de 32 bits, como se muestra en la figura.



Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Si dos hosts tienen el mismo patrón de bits en la porción de red especificada de la secuencia de 32 bits, esos dos hosts residen en la misma red.

¿Pero cómo saben los hosts qué porción de los 32 bits identifica la red y qué porción identifica el host? El rol de la máscara de subred.

6.1.2 La Máscara de Subred

Como se muestra en la figura 1, asignar una dirección IPv4 a un host requiere lo siguiente:

- **Dirección** única del host.
- **Máscara de** parte de

Nota: Se requiere una (gateway) remotas y se requieren para traducir nombres

La máscara de subred porción de red de la IPv4. Cuando se dispositivo, la máscara dirección de red del representa todos los

La siguiente figura 32 bits en formato Observe cómo la secuencia consecutiva

Máscara de Subred	Dirección de 32 bits	Longitud del Prefijo
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

IPv4: Esta es la dirección IPv4

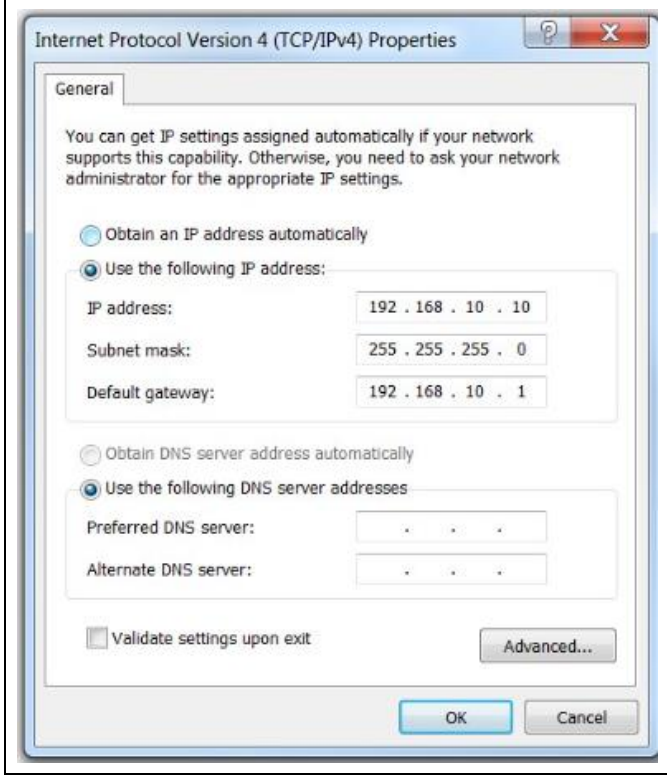
subred: Se usa para identificar la red/host de la dirección IPv4.

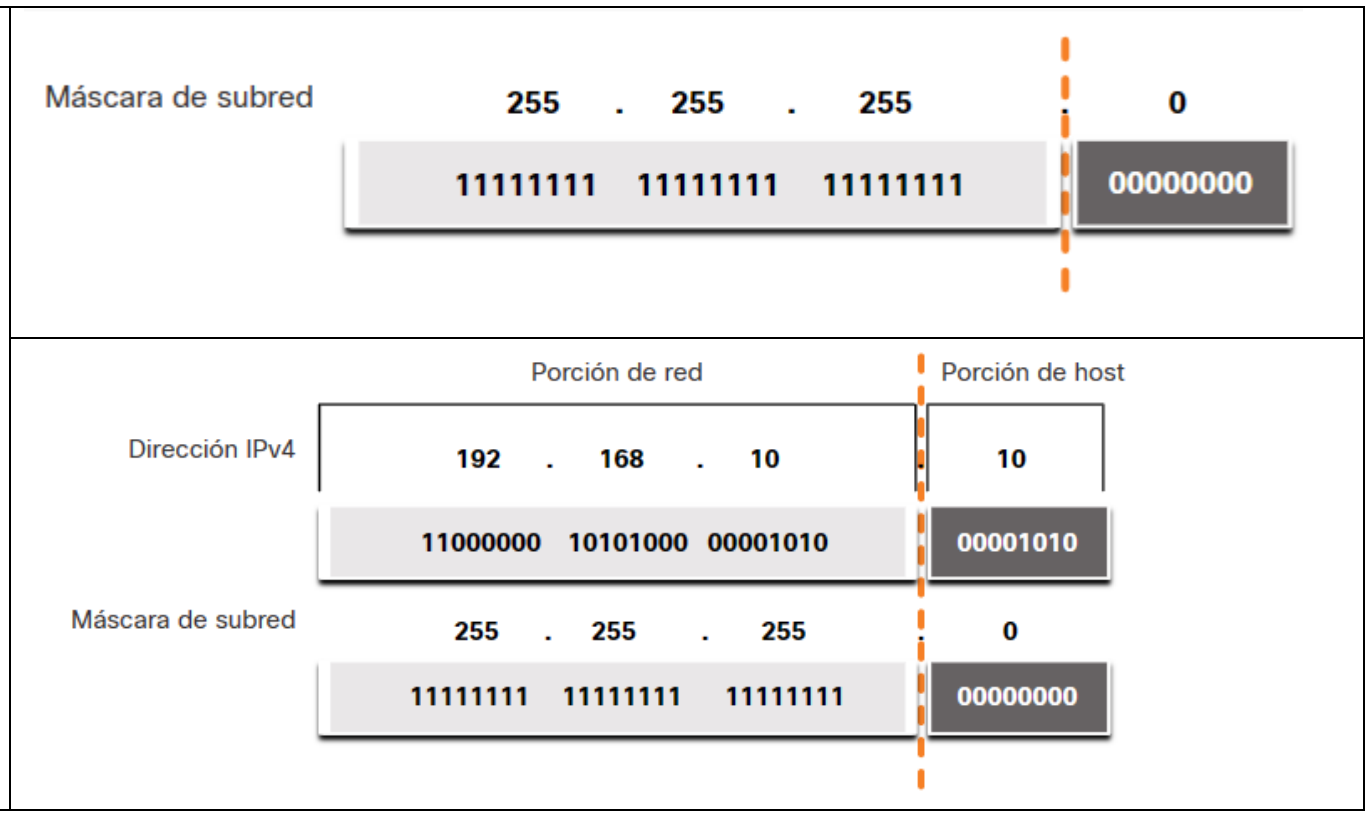
dirección IPv4 de puerta de enlace predeterminada para llegar a redes direcciones IPv4 del servidor DNS de dominio a direcciones IPv4.

IPv4 se usa para diferenciar la porción de host de una dirección asigna una dirección IPv4 a un de subred se usa para determinar la dispositivo. La dirección de red dispositivos de la misma red.

muestra la máscara de subred de decimal y binario punteado. máscara de subred es una de bits "1" seguida de una de bits "0".

Para identificar las porciones de red y host de una dirección IPv4, la máscara de subred se compara con la dirección IPv4 bit por bit, de izquierda a derecha como se muestra en la figura 3. Tenga en cuenta que la máscara de subred en realidad no contiene la porción de red o host de una dirección IPv4, solo le dice a la computadora dónde buscar la parte de la dirección IPv4 que es la porción de red y qué parte es la porción de host. El proceso real que se usa para identificar la porción de red y la porción de host se denomina AND.





6.1.3 La Longitud del Prefijo

Puede ser difícil expresar direcciones de red y de host con la dirección de la máscara de subred decimal punteada. Afortunadamente, hay un método alternativo para identificar una máscara de subred, un método llamado longitud del prefijo.

La longitud del prefijo es el número de bits establecidos en 1 en la máscara de subred. Está escrito en "notación de barra", que se observa mediante una barra diagonal (/) seguida del número de bits establecidos en 1. Por lo tanto, cuente el número de bits en la máscara de subred y anteponga una barra diagonal.

Consulte la tabla para ver ejemplos. En la primera columna, se enumeran varias máscaras de subred que se pueden usar con una dirección de host. En la segunda columna, se muestra la dirección binaria de 32 bits convertida. En la última columna, se muestra la longitud de prefijo resultante.

Nota: Una dirección de red también se conoce como prefijo o prefijo de red. Por lo tanto, la longitud del prefijo es el número de bits "1" en la máscara de subred.

Al representar una dirección IPv4 utilizando una longitud de prefijo, la dirección IPv4 se escribe seguida de la longitud del prefijo sin espacios. Por ejemplo, 192.168.10.10 255.255.255.0 se escribiría como 192.168.10.10/24. Más adelante se analiza el uso de varios tipos de longitudes de prefijo. Por ahora, el foco estará en el prefijo / 24 (es decir, 255.255.255.0)

6.1.4 Determinación de la Red: AND lógico

Un AND lógico es una de las tres operaciones booleanas utilizadas en la lógica booleana o digital. Las otras dos son OR y NOT. La operación AND se usa para determinar la dirección de red. El AND lógico es la comparación de dos bits que producen los resultados que se muestran a continuación. Observe que solo mediante 1 AND 1 se obtiene 1. Cualquier otra combinación da como resultado un 0.

- 1 Y 1 = 1
- 0 Y 1 = 0

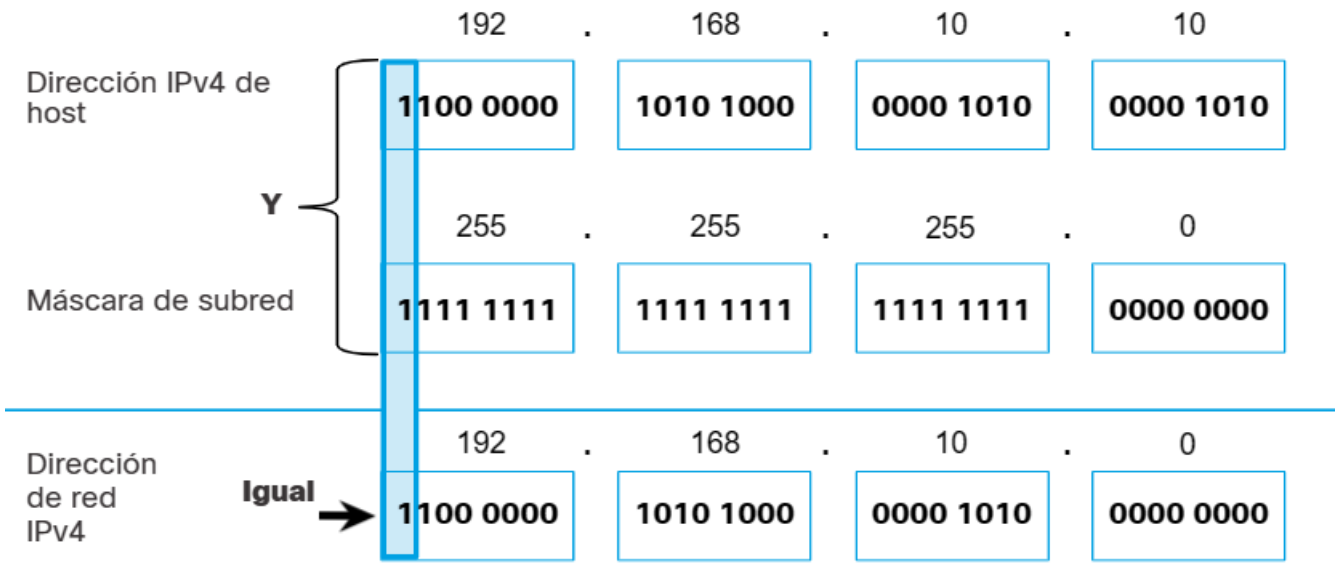
- 1 Y 0 = 0
- 0 Y 0 = 0

Nota: En la lógica digital, 1 representa True y 0 representa False Cuando se utiliza una operación AND, ambos valores de entrada deben ser True (1) para que el resultado sea True (1).

Para identificar la dirección de red de un host IPv4, se recurre a la operación lógica AND para la dirección IPv4, bit por bit, con la máscara de subred. El uso de la operación AND entre la dirección y la máscara de subred produce la dirección de red.

Para ilustrar cómo se usa AND para descubrir una dirección de red, considere un host con dirección IPv4 192.168.10.10 y una máscara de subred de 255.255.255.0, como se muestra en la figura:

- **Dirección de hostIPv4 (192.168.10.10)** - La dirección IPv4 del host en formato decimal y binario punteados.
- **Máscara de subred (255.255.255.0)** - La máscara de subred del host en formatos decimales y binarios punteados.
- **Dirección de red (192.168.10.0)** - La operación AND lógica entre la dirección IPv4 y la máscara de subred da como resultado una dirección de red IPv4 que se muestra en formato decimal y binario punteados.



Utilizando la primera secuencia de bits como ejemplo, observe que la operación AND se realiza en el bit 1 de la dirección del host con el bit 1 de la máscara de subred. Esto resulta en un bit "1" para la dirección de red. 1 AND 1 = 1.

La operación AND entre una dirección de host IPv4 y una máscara de subred da como resultado la dirección de red IPv4 para este host. En este ejemplo, la operación AND entre la dirección host 192.168.10.10 y la máscara de subred 255.255.255.0 (/24) da como resultado la dirección de red IPv4 192.168.10.0/24. Esta es una operación IPv4 importante, ya que le dice al host a qué red pertenece.

6.1.5 Video - Direcciones de Red, Host y Difusión.

Todos los dispositivos en una red IPv4 necesitan una dirección lógica de 32 bits para poder comunicarse. Esta dirección lógica de host IPv4 de 32 bits consiste en una porción de red o **ID de red** a la izquierda y una porción de host o **ID de host** a la derecha. La longitud de estos depende del tamaño de la red, en redes más grandes tendremos una porción de host más larga. Se puede pensar en una red como un rango de direcciones. Todos los dispositivos en la misma red tienen el mismo patrón de bits para su ID de red, pero tendrán una ID de host diferente. Algunas direcciones en este rango están reservadas y tienen un nombre y significado especial. Por ejemplo, la primera dirección del rango se utiliza para identificar la propia red y no se puede asignar a ningún host. Se conoce como la dirección de red. La última en el rango se llama dirección de broadcast o de transmisión y se usa para enviar un mensaje a todos los dispositivos en la red a la vez, tampoco se puede asignar a ningún host. Todas las direcciones IP entre la de red y las direcciones de transmisión conforman el rango de host utilizable o válido y se usan para dirigirse a los hosts en la red. Echemos un vistazo a cómo se determinan estas direcciones. Para reenviar datos, un dispositivo necesita saber. ¿En qué red está? Usando su dirección IP de host, su máscara de subred y un proceso llamado Binary ANDing un dispositivo puede encontrar lo que se denomina dirección de red. Esta dirección representa la red a la que pertenece el host y será ligeramente diferente de su IP de host. Para hacer esto, el dispositivo compara su IP de host y su máscara de subred bit por bit, si los valores de bit son binarios, el resultado es binario. Si uno o ambos valores de bit es 0, el resultado es un cero binario. Echemos un vistazo a un ejemplo. Digamos que tenemos una PC con una dirección IP de host y una máscara de subred de 192.168.2.38/24 y usaremos ANDing para encontrar la dirección de red del host. Aquí está la IP del host y el binario. Aquí está la máscara de subred y el binario. Si los comparamos bit por bit, podemos ver. Que 1 y 1 dan como resultado 1, 1 y 1 da como resultado 1, 0 y 1 da como resultado 0, 0 y 1 da como resultado 0, y así sucesivamente hasta que hayamos comparado los 32 bits. Observe que el último octeto es todo ceros binarios debido a que estamos usando una máscara de subred /24, los primeros tres octetos representan la parte de la red y el último octeto es la parte del host. Las direcciones de red siempre tendrán ceros binarios en toda su porción de host, sin importar cuán largos sean. En este caso, los últimos ocho bits si los convertimos a decimal, podemos ver que este host pertenece a la red 192.168.2.0/24. Ahora determinemos la dirección de transmisión para esta red, que se usa para enviar un mensaje a todos los dispositivos en la red a la vez. Mientras que la dirección de red tenía todos ceros binarios en la parte del host, la dirección de transmisión tendrá todos unos binarios, ya que la parte del host en este ejemplo es solo el último octeto para determinar la dirección de transmisión. Mantenemos la parte de la red igual y cambiamos el porción de host a todos los binarios. Esto da como resultado una dirección de transmisión de 192.168.2.255. A continuación, determinaremos las direcciones de host utilizables que se encuentran entre la red y las direcciones de transmisión. El primer host utilizable en binario será todo ceros binarios, con un 1 binario al final de la parte del host, que se convierte en decimal con puntos. Esto nos dice que el primer host utilizable en esta red es **192.168.2.1**. Por último, determinaremos el último host utilizable, que serán todos 1s binarios con un cero al final. El patrón de bits opuesto del primer host utilizable. Convirtiendo a decimal con puntos, obtenemos **192.168.2.254**. Recapitulemos nuestros cálculos. Comenzamos con la dirección IP del host de 192.168.2.38/24. Usando el ANDing binario, determinamos que este host pertenece a la red 192.168.2.0. Manteniendo la parte de la red igual, pero colocando todos los 1 binarios en la porción de host determinamos que la dirección de transmisión para esta red es 192.168.2.255. Una vez más, manteniendo la parte de la red igual, pero cambiando la parte del host, determinamos que el rango de host utilizable para asignar direcciones a dispositivos en esta red es 192.168.2.1, que es un 1 por encima de la dirección de red, y 192.168.2.254, que es un 1 por debajo de la dirección de transmisión. Puede ver que nuestra dirección IP de host original se encuentra dentro de este rango. Cosas a tener en cuenta cuando se trabaja con direcciones IPv4. Todas las direcciones de host IPv4 tienen una longitud de 32 bits, una parte de la dirección representa la red a la que pertenece el host y comienza a la izquierda. La parte restante es la parte del host que identifica al host en la red. Dos direcciones especiales reservadas en cada red que no se pueden asignar a hosts: Una es la dirección de red, que es la más baja en el rango de direcciones y representa la red a la que pertenecen todos los dispositivos, y la otra es la dirección de transmisión, que es la dirección más alta en el rango y se puede usar para saludar a todos los host en la red a la vez. Afortunadamente, hay atajos que puede tomar para calcular estas direcciones sin tener que convertir a binario primero, pero examinar estas direcciones a nivel de bit debería ayudarlo a comprender cómo los dispositivos de red las interpretan y también cómo se deriva el formato decimal con puntos.

IPv4 Addressing

- IPv4 addresses are 32-bit logical addresses
- Consist of a network portion and a host portion
  - Length will vary depending on the size of the network
- A network is a range of addresses
  - All devices on the same network have the same network portion (network ID) but a different host portion (host ID)

Determining the Network Address

- Given the host IPv4 address and subnet mask 192.168.2.38/24, use ANDing to find the network address of the host.
  - /24 subnet mask equals 255.255.255.0

Network Portion | /24 | Host Portion

Host IP Address	11000000	10101000	00000010	00100110
Subnet Mask	11111111	11111111	11111111	00000000
Network Address	11000000	10101000	00000010	00000000

Network Address = **192.168.2.0/24**

Determining the Broadcast Address

- Used to send a message to all devices on the network at once.
  - Keep the network portion the same
  - Place all binary 1s in the host portion (since the host portion in this example is just the last octet, change all bits in last octet to 1s)
- Convert to dotted-decimal

Network Portion | /24 | Host Portion

Network Address	11000000	10101000	00000010	00000000
Broadcast Address	11000000	10101000	00000010	11111111
Broadcast Address Dotted-Decimal	192	168	2	255

- Broadcast Address for this network is **192.168.2.255**

Determining the First Usable Host Address

- Usable host addresses lie between the network address and the broadcast address
- First usable host in binary will be all binary 0s with a binary 1 at the end of the host portion, then convert to dotted-decimal.

Network Portion | /24 | Host Portion

Network Address	11000000	10101000	00000010	00000000
First Usable Host Address	11000000	10101000	00000010	00000001
First Usable Host Dotted-Decimal	192	168	2	1

- First usable host for this network is **192.168.2.1**

To Recap Our Calculations

- Given the host IP address of 192.168.2.38/24, we determined:

Network Address	First Usable Host	Last Usable Host	Broadcast Address
192.168.2.0	192.168.2.1	192.168.2.254	192.168.2.255

192.168.2.38
(falls within the range of usable host addresses)

6.1.6 Actividad - Uso del AND para Determinar la Dirección de Red

Utilice la operación AND para determinar la dirección de red (en formatos binario y decimal).

Dirección del servidor	10	254	160	122
Máscara de subred	255	255	255	128
Dirección de host en binario	00001010	11111110	10100000	01111010
Máscara de subred en binario	11111111	11111111	11111111	10000000
Dirección de red en binario	00001010	11111110	10100000	00000000
Dirección de red en decimal	10	254	160	0

Dirección del servidor	10	176	143	95
Máscara de subred	255	255	255	254
Dirección de host en binario	00001010	10110000	10001111	01011111
Máscara de subred en binario	11111111	11111111	11111111	11111110
Dirección de red en binario	00001010	10110000	10001111	01011110
Dirección de red en decimal	10	176	143	94

Dirección del servidor	10	59	31	188
Máscara de subred	255	255	0	0
Dirección de host en binario	00001010	00111011	00011111	10111100
Máscara de subred en binario	11111111	11111111	00000000	00000000
Dirección de red en binario	00001010	00111011	00000000	00000000
Dirección de red en decimal	10	59	0	0

Dirección del servidor	10	28	163	95
Máscara de subred	255	255	255	252
Dirección de host en binario	00001010	00011100	10100011	01011111
Máscara de subred en binario	11111111	11111111	11111111	11111100
Dirección de red en binario	00001010	00011100	10100011	01011100
Dirección de red en decimal	10	28	163	92

6.1.7 Verifique su Comprensión - Estructura de la Dirección IPv4

El Host-A tiene la dirección IPv4 y la máscara de subred 10.5.4.100 255.255.255.0. ¿Cuál es la dirección de red del Host-A?

10.0.0.0	10.5.0.0	10.5.4.0 ☺←	10.5.4.100

El host A tiene la dirección IPv4 y la máscara de subred 172.16.4.100 255.255.0.0. ¿Cuál es la dirección de red del host A?

172.0.0.0	172.16.0.0 ☺←	172.16.4.0	172.16.4.100

El Host-A tiene la dirección IPv4 y la máscara de subred 10.5.4.100 255.255.255.0. ¿Cuál de las siguientes direcciones IPv4 estaría en la misma red que el Host-A? (Seleccione todas las opciones que correspondan)

10.5.4.1 ☺←	10.5.0.1	10.5.4.99 ☺←	10.0.0.98	10.5.100.4

El host A tiene la dirección IPv4 y la máscara de subred 172.16.4.100 255.255.0.0. ¿Cuál de las siguientes direcciones IPv4 estaría en la misma red que el Host-A? (Seleccione todas las opciones que correspondan)

172.16.4.99 ☺←	172.16.0.1 ☺←	172.17.4.99	172.17.4.1	172.18.4.1

El Host-A tiene la dirección IPv4 y la máscara de subred 192.168.1.50 255.255.255.0. ¿Cuál de las siguientes direcciones IPv4 estaría en la misma red que el Host-A? (Seleccione todas las opciones que correspondan)

192.168.0.1	192.168.0.100	192.168.1.1 ☺←	192.168.1.100 ☺←	192.168.2.1

2. Resumen de direccionamiento IPv4

6.2.1 ¿Qué Aprendí en este Módulo?

Estructura de la Dirección IPv4

Una dirección IPv4 es una dirección jerárquica de 32 bits que se compone de una porción de red y una porción de host. Al determinar la porción de red frente a la porción de host, debe mirar la secuencia de 32 bits. Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Si dos hosts tienen el mismo patrón de bits en la porción de red especificada de la secuencia de 32 bits, esos dos hosts residen en la misma red.

La máscara de subred IPv4 se usa para diferenciar la porción de red de la porción de host de una dirección IPv4. Cuando se asigna una dirección IPv4 a un dispositivo, la máscara de subred se usa para determinar la dirección de red del dispositivo. La dirección de red representa todos los dispositivos de la misma red.

Un método alternativo para identificar una máscara de subred, un método llamado longitud de prefijo. La longitud del prefijo es el número de bits establecidos en 1 en la máscara de subred. Está escrito en "notación de barra", que se observa mediante una barra diagonal (/) seguida del número de bits establecidos en 1. Por ejemplo, 192.168.10.10 255.255.255.0 se escribiría como 192.168.10.10/24.

La operación AND se usa para determinar la dirección de red. La operación lógica AND es la comparación de dos bits. Observe que solo mediante 1 AND 1 se obtiene 1. Cualquier otra combinación da como resultado un 0.

- 1 Y 1 = 1
- 0 Y 1 = 0
- 1 Y 0 = 0
- 0 Y 0 = 0

Para identificar la dirección de red de un host IPv4, se recurre a la operación lógica AND para la dirección IPv4, bit por bit, con la máscara de subred. El uso de la operación AND entre la dirección y la máscara de subred produce la dirección de red.

6.2.2 Webster - Preguntas de Reflexión

Antes de tomar este módulo, me sentía como Marcy y Vincent. No tenía una buena idea de cómo los números en la dirección IPv4 eran importantes. ¿Conocía la dirección jerárquica de 32 bits que se compone de una parte de red y una parte de host? ¿Puede explorar esto en su propia red? ¿Y quién sabía de ANDing y la máscara de subred?

Me siento un poco más como Bob después de este módulo y espero que usted también.

6.2.3 Prueba de Direccionamiento IPv4

¿Qué enunciado describe el direccionamiento IPv4?

Los enrutadores utilizan la dirección IP de 32 bits completa para determinar la ubicación de cada host individual.
La porción de red de una dirección IP de destino se obtiene realizando una operación AND entre una dirección IP de host y una máscara de subred. ☺←
Una dirección IPv4 consta de dos partes: una parte de red y una parte de subred.
Dos hosts con la misma máscara de subred están en la misma red.

¿Qué enunciado describe un propósito de la configuración de la máscara de subred para un host?

Se utiliza para describir el tipo de subred.
Se utiliza para identificar la puerta de enlace predeterminada.
Se utiliza para determinar a qué red está conectado el host. ☺←
Se utiliza para determinar la cantidad máxima de bits dentro de un paquete que se puede colocar en una red en particular.

¿Cuántos octetos hay en una dirección IPv4?

4 ☺←	8	16	32

¿Qué rango completo de valores decimales es válido en un octeto de una dirección IPv4?

0a 31	1 a 64	0 a 128	0 a 255 ☺←	1 a 256

¿Con qué propósito se utilizan las direcciones IPv4?

Una dirección IPv4 se utiliza para identificar de forma única un dispositivo en una red IP. ☺←
Una dirección IPv4 se graba en la tarjeta de red para identificar de forma única un dispositivo.
Una dirección IPv4 se utiliza para identificar de forma única la aplicación que solicitó la información de un dispositivo remoto.
Se utiliza una dirección IPv4 para identificar el número de redes IP disponibles.

¿Cuál es la notación de longitud de prefijo para la máscara de subred 255.255.255.224?

/25	/26	/27 ☺←	/28

¿Qué dos partes son componentes de una dirección IPv4? (Escoja dos opciones).

porción de subred
porción de red ☺←

- porción lógica
- porción de host ☺←
- porción física
- porción de difusión

¿Qué se obtiene al agregar (ANDing) la dirección 192.168.65.3/18 con su máscara de subred?

192.168.0.0	192.168.16.0	192.168.32.0	192.168.64.0 ☺←

¿Qué tienen en común los dispositivos de la misma subred IPv4?

- Todos usan la misma puerta de enlace predeterminada. ☺←
- Todos tienen una máscara de subred de /8, /16 o /24.
- Todos tienen el mismo último octeto en sus direcciones IPv4.
- Todos tienen el mismo número en los primeros tres octetos de su dirección IPv4.

¿Cuántas direcciones exclusivas hay disponibles para asignar a hosts en la red de 10.100.16.0 con la máscara de subred 255.255.252.0?

254	510	1022 ☺←	494

Explique: Una máscara 255.255.252.0 equivale a un prefijo /22. Un prefijo de /22 proporciona 22 bits para la porción de red y deja 10 bits para la porción de host. Los 10 bits de la porción de host proporcionan 1022 direcciones IP utilizables (2^10 – 2 = 1022).

¿Cuál es una dirección de puerta de enlace predeterminada válida para un host configurado con la dirección IP 10.25.1.110 y una máscara de subred 255.255.255.192?

10.25.1.65 ☺←	10.25.1.1	10.0.0.1	10.25.1.127

Cuando el direccionamiento IPv4 se configura manualmente en un servidor web, ¿cuál es la propiedad de la configuración IPv4 que identifica las porciones de red y de host de una dirección IPv4?

Dirección del servidor DNS	Máscara de subred ☺←	Puerta de enlace predeterminada	Dirección del servidor DHCP

Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 4 – 6

Bienvenido al Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 4 - 6.

Esta evaluación cubre los conceptos básicos y las habilidades presentadas en los Módulos 4 a 6 del curso Dispositivos de Red y Configuración Inicial. Hay 21 preguntas en total. Debe alcanzar el 70% para aprobar este examen.

Tiene intentos ilimitados para aprobar el examen. Se proporcionan comentarios para dirigirlo a áreas que pueden requerir atención adicional.

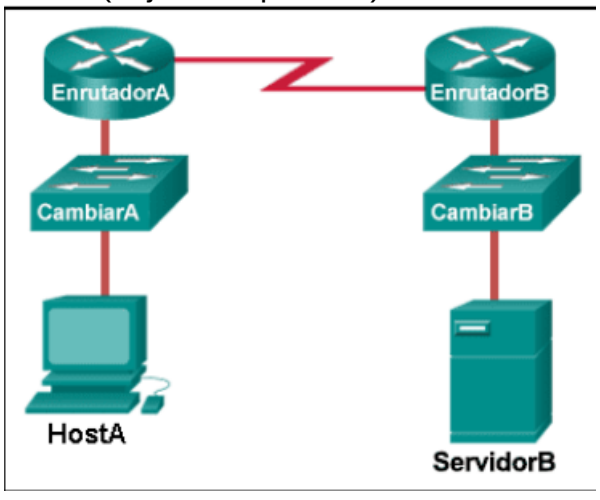
El contenido de Cisco Networking Academy está protegido por leyes de derechos de autor. Además, está prohibido publicar, distribuir o compartir el contenido de este examen sin autorización.

© 2022, Cisco Systems, Inc.

¿Qué información utiliza un conmutador para mantener actualizada la información de la tabla de direcciones MAC?

- la dirección MAC de origen y el puerto de entrada ☺←
- las direcciones MAC de origen y destino y el puerto de entrada
- las direcciones MAC de origen y destino y el puerto de salida
- la dirección MAC de destino y el puerto de entrada
- la dirección MAC de destino y el puerto de salida
- la dirección MAC de origen y el puerto de salida

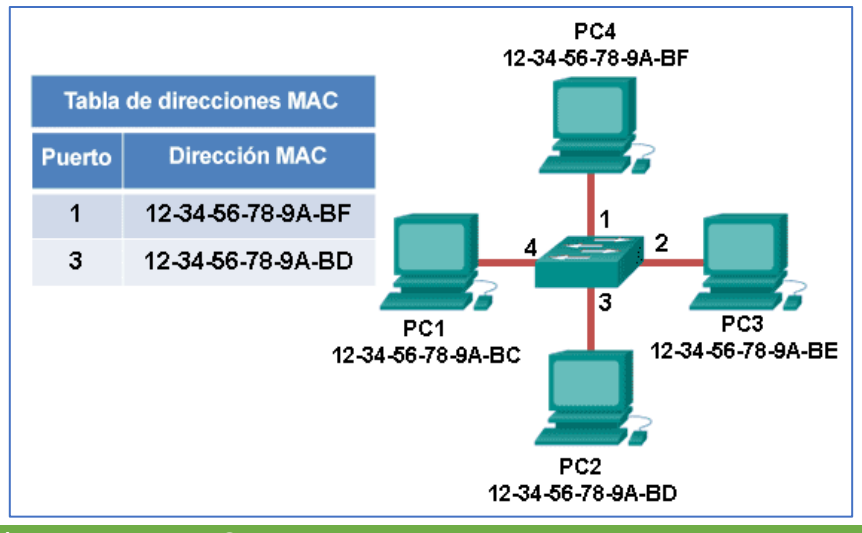
Observe la ilustración. El Servidor B está intentando ponerse en contacto con HostA. ¿Qué dos instrucciones identifican correctamente el direccionamiento que Servidor B generará en el proceso? (Elija dos opciones).



- ServidorB generará una trama con la dirección MAC de destino del SwitchB.
- ServidorB generará una trama con la dirección MAC de destino de RouterA.
- ServidorB generará un paquete con la dirección IP de destino de HostA. ☺←
- ServidorB generará un paquete con la dirección IP de destino de RouterA.
- ServidorB generará una trama con la dirección MAC de destino del RouterB. ☺←
- ServidorB generará un paquete con la dirección IP de destino del RouterB.

Explique: Para enviar datos a HostA, ServidorB generará un paquete que contiene la dirección IP del dispositivo de destino en la red remota y una trama que contiene la dirección MAC del dispositivo de puerta de enlace predeterminado en la red local.

Observe la ilustración. En la ilustración, se muestra una pequeña red conmutada y el contenido de la tabla de direcciones MAC del switch. La PC1 envió una trama dirigida a la PC3. ¿Qué hará el switch con la trama?



El switch reenviará la trama solamente a los puertos 1 y 3.
El switch reenviará la trama a todos los puertos, excepto al puerto 4. ☺←
El switch descartará la trama.
El switch reenviará la trama solamente al puerto 2.
El switch reenviará la trama a todos los puertos.

Abra la actividad de PT. Realice las tareas en las instrucciones de la actividad y luego responda la pregunta. ¿Cuál puerto es usado cuando Switch0 envía tramas a un host con la dirección IPv4?

Fa0/11 ☺←	Fa0/5	Fa0/1	Fa0/9

¿Cuándo registraría un conmutador varias entradas para un solo puerto de conmutador en su tabla de direcciones MAC?

cuando un enrutador está conectado al puerto del conmutador
cuando se han reenviado varias transmisiones ARP
cuando otro conmutador está conectado al puerto del conmutador ☺←
cuando el conmutador está configurado para conmutación de capa 3

Observe la ilustración. Se emite un ping a PC3 desde PC0, PC1 y PC2 en este orden exacto. ¿Qué direcciones MAC se incluirán en la tabla de direcciones MAC de S1 que está asociada con el puerto Fa0/1?

solo la dirección MAC de la PC1
solo direcciones MAC PC0 y PC1 ☺←
solo la dirección MAC de la PC2
solo la dirección MAC de PC0
PC0, PC1 y PC2

Cuando una computadora ensambla una trama que se debe enviar por la red, ¿cuál es el tamaño máximo de una trama de Ethernet?

128 bytes	1518 bytes ☺←	1024 bytes	64 bytes

¿Qué campo de encabezado IPv6 se utiliza para indicar el protocolo de capa superior o el encabezado de extensión incluido en el paquete?

Clase de tráfico	Siguiente encabezado ☺←	Longitud de carga útil	Etiqueta de flujo

Haga coincidir las características con la versión correcta del protocolo IP.

12 campos de encabezado básicos	Espacio de direcciones de 128 bits	Encabezado de 40 octetos	Encabezado de 20 octetos	8 campos del encabezado	Espacio de direcciones de 32 bits
IPv4	IPv6	IPv6	IPv4	IPv6	IPv4

¿Qué campo en un paquete IPv6 utiliza el router para determinar si un paquete ha caducado y debe descartarse?

No hay ruta para el destino	No se puede alcanzar la dirección	Límite de saltos ☺←	TTL

¿Qué es correcto en relación con NAT para IPv6?

NAT64 ha sido desaprobado por IETF a favor de NAT-PT.
Se utiliza para traducir las direcciones IPv6 privadas a direcciones IPv6 públicas.
Es un mecanismo temporal para ayudar en la migración de IPv4 a IPv6. ☺←
La pila dual es un ejemplo de implementación de NAT para IPv6.

¿Cuáles son las dos funciones que proporciona la capa de red? (Elija dos opciones).

transporte de datos entre procesos que se ejecutan en hosts de origen y de destino
dirigir paquetes de datos a hosts de destino en otras redes ☺←
proporcionando conexiones de extremo a extremo exclusivas
colocar datos en el medio de red
proporcionando a los dispositivos finales un identificador de red único ☺←

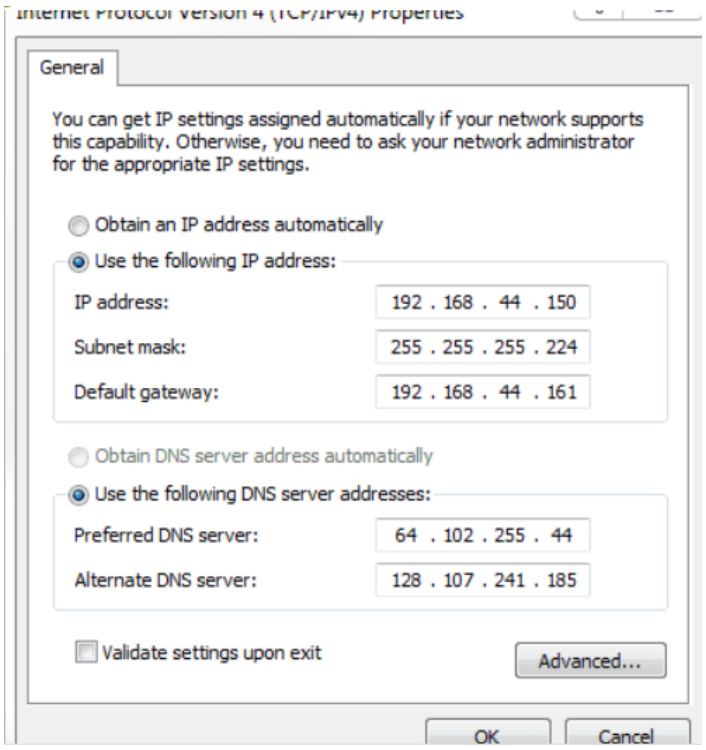
¿Cuál campo del encabezado IPv4 es responsable de definir la prioridad del paquete?

Señaladores	Identificador de flujo	Servicios diferenciados ☺←	Clase de tráfico

¿Cuál es una de las ventajas que ofrece el encabezado de IPv6 simplificado sobre el IPv4?

- Manejo eficaz de paquetes ☺←
- Pocos requisitos de procesamiento de checksums
- Direcciones IP de origen y destino de menor tamaño
- Encabezado de menor tamaño

Observe la ilustración. Una computadora configurada con la dirección IPv4 como se muestra en la ilustración no puede acceder a Internet. ¿Cuál es el problema?



- La dirección IP es una dirección de red
- Las configuraciones no son validadas
- La dirección de la puerta de enlace está en la subred incorrecta ☺←
- La dirección IP es una dirección de difusión

Considere el grupo de cinco direcciones IPv4, cada una con la máscara de subred 255.255.255.0. ¿Cuáles dos direcciones IPv4 pertenecen a la misma red local? (Elija dos opciones).

192.167.10.74	192.168.10.2 ☺←	192.168.100.62	193.168.10.16	192.168.10.56 ☺←

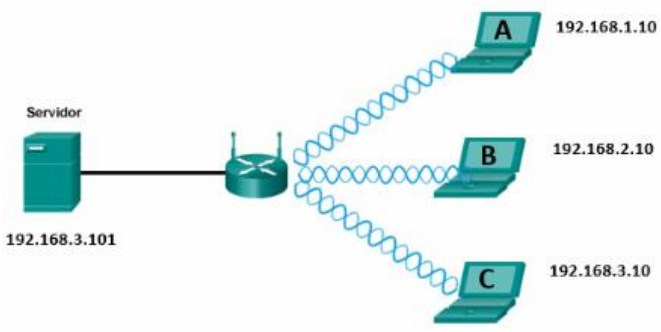
¿Cuáles dos hosts existen en la misma subred? (Escoja dos opciones).

172.16.100.4/23 ☺←	172.16.97.78/23	172.16.101.199/23 ☺←	172.16.98.250/23	172.16.102.237/23

¿Qué máscara de subred se asociaría con el prefijo IPv4 de /28?

255.255.255.0	255.255.255.224	255.255.255.248	255.255.255.240 ☺←	255.255.255.252

Observe la ilustración. Si todos los dispositivos usan una máscara de subred 255.255.255.0, ¿qué computadora portátil tendría una dirección IP con el mismo número de red que el servidor?

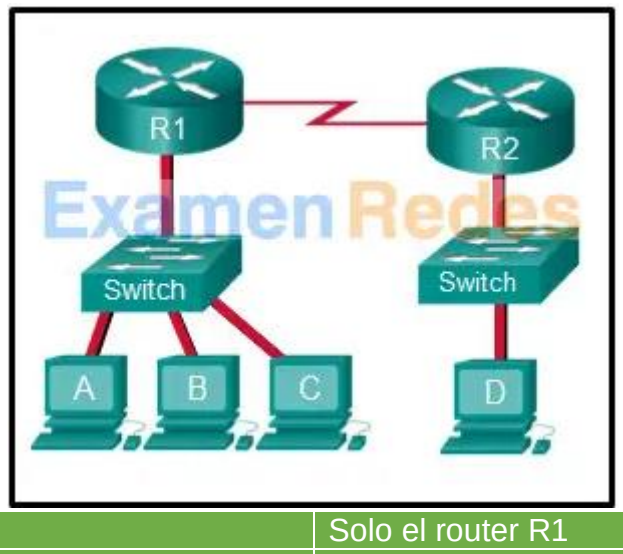


C ☺←	B	A

¿Por qué un dispositivo de capa 3 realiza el proceso AND en una dirección IP y en una máscara de subred de destino?

- Para identificar las tramas defectuosas
- Para identificar la dirección de red de la red de destino ☺←
- Para identificar la dirección de difusión de la red de destino
- Para identificar la dirección del host de destino

Observe la ilustración. Los switches tienen una configuración predeterminada. El host A debe comunicarse con el host D, pero no tiene la dirección MAC de la puerta de enlace predeterminada. ¿Cuáles dispositivos de red recibirán la solicitud ARP que fue enviada por el host A?



Solo los hosts A, B, C y D	Solo el router R1
Solo los hosts B y C	Solo el host D
Solo los hosts A, B y C	Solo el router R1 y los hosts B y C ☺←

¿Qué campo en el encabezado IPv6 apunta a la información de capa de red opcional que se incluye en el paquete IPv6?

Version	Encabezado siguiente ☺←
Identificador de flujo	Clase de trafico

Explique: La información opcional de capa 3 sobre la fragmentación, la seguridad y la movilidad se incluye en los encabezados de extensión de un paquete IPv6. El encabezado siguiente del encabezado IPv6 apunta a estos encabezados de extensión opcionales si están presentes.

Un ingeniero de redes divide la red 192.168.100.0 /24 en 16 subredes. ¿Cuántas direcciones de host utilizables estarán disponibles en cada una de las subredes?

30	6	62	14 ☺←

Módulo 7: Resolución de dirección

0. Introducción

7.0.1 Webster - ¿Por Qué Debería Tomar este Módulo?

¡Webster aquí otra vez! Tengo otro amigo que presentarles. Se llama Olcay. Olcay es profesional de TI en una empresa de energía en Turquía. Está asesorando a un nuevo empleado llamado Abay. Abay estará siguiendo a Olcay durante el próximo mes para ser más hábil en redes en la empresa de energía. Olcay le pregunta a Abay qué sabe sobre la resolución de direcciones. Abay sabe que para enviar un paquete a otro host en la misma red IPv4 local, un host debe conocer la dirección IPv4 y la dirección MAC del dispositivo de destino. Un dispositivo utiliza ARP para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4.

Si Abay va a tener éxito en su nuevo trabajo, debe aprender un poco más y usted también. Le sugiero que tome este módulo sobre Resolución de Direcciones.

7.0.2 ¿Qué Voy a Aprender en este Módulo?

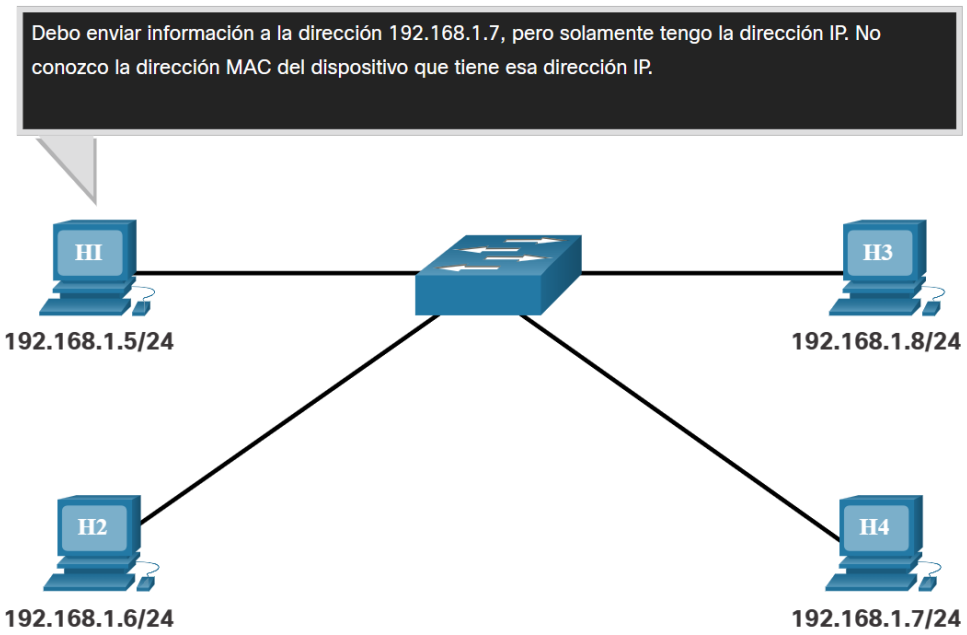
- Título del Módulo: Resolución de Direcciones
- Objetivo del Módulo: Explicar cómo ARP permite la comunicación en una red de área local.

Título del Tema	Objetivo del Tema
ARP	Describa el propósito de ARP.

1. ARP

7.1.1 Descripción General de ARP

Si su red utiliza el protocolo de comunicaciones IPv4, el protocolo de resolución de direcciones o ARP es lo que necesita para asignar direcciones IPv4 a direcciones MAC. En este tema se explica cómo funciona ARP.



Cada dispositivo IP de una red Ethernet tiene una dirección MAC Ethernet única. Cuando un dispositivo envía una trama de capa 2 de Ethernet, contiene estas dos direcciones:

- **Dirección MAC de destino** - La dirección MAC Ethernet del dispositivo de destino en el mismo segmento de red local. Si el host de destino está en otra red, entonces la dirección de destino en el trama sería la del gateway predeterminado (es decir, router).
- **Dirección MAC de origen** - La dirección MAC de la NIC de Ethernet en el host de origen.

La figura ilustra el problema al enviar una trama a otro host en el mismo segmento en una red IPv4.

Para enviar un paquete a otro host en la misma red IPv4 local, un host debe conocer la dirección IPv4 y la dirección MAC del dispositivo de destino. Las direcciones IPv4 de destino del dispositivo se conocen o se resuelven por el nombre del dispositivo. Sin embargo, las direcciones MAC deben ser descubiertas.

Un dispositivo utiliza el Protocolo de resolución de direcciones (ARP) para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4. ARP proporciona dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC
- Mantener una tabla de asignaciones de direcciones IPv4 a MAC

7.1.2 Funciones de ARP

Cuando se envía un paquete a la capa Enlace de Datos para encapsularlo en una trama de Ethernet, el dispositivo consulta una tabla en su memoria para encontrar la dirección MAC que está asignada a la dirección IPv4. Esta tabla se almacena temporalmente en la memoria RAM y se denomina tabla ARP o caché ARP.

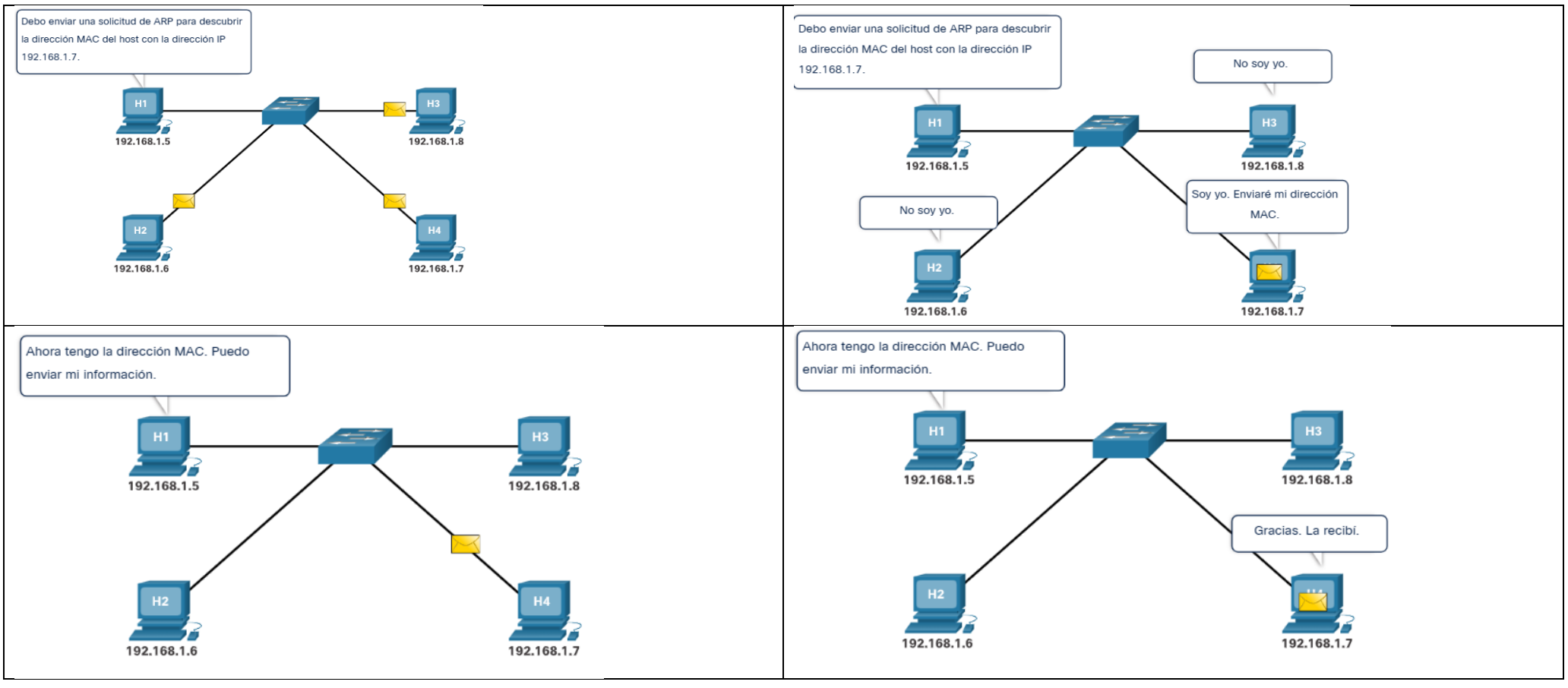
El dispositivo emisor busca en su tabla ARP la dirección IPv4 de destino y la dirección MAC correspondiente.

- Si la dirección IPv4 de destino del paquete está en la misma red que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 de destino en la tabla ARP.
- Si la dirección IPv4 de destino está en una red diferente que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 del gateway predeterminado.

En ambos casos, se realiza una búsqueda de la dirección IPv4 y la dirección MAC correspondiente para el dispositivo destino.

En cada entrada o fila de la tabla ARP, se enlaza una dirección IPv4 con una dirección MAC. La relación entre los dos valores se denomina asignación. Esto solamente significa que es posible buscar una dirección IPv4 en la tabla y encontrar la dirección MAC correspondiente. La tabla ARP almacena temporalmente (en caché) la asignación para los dispositivos de la LAN.

Si el dispositivo localiza la dirección IPv4, se utiliza la dirección MAC correspondiente como la dirección MAC de destino de la trama. Si no se encuentra ninguna entrada, el dispositivo envía una solicitud de ARP.



7.1.3 Video - Operación de ARP - Solicitud de ARP

Se envía una solicitud ARP ***(ARP REQUEST***) cuando un dispositivo necesita la dirección MAC asociada con una dirección IPv4, y no tiene una entrada para la dirección IPv4 en su tabla ARP.

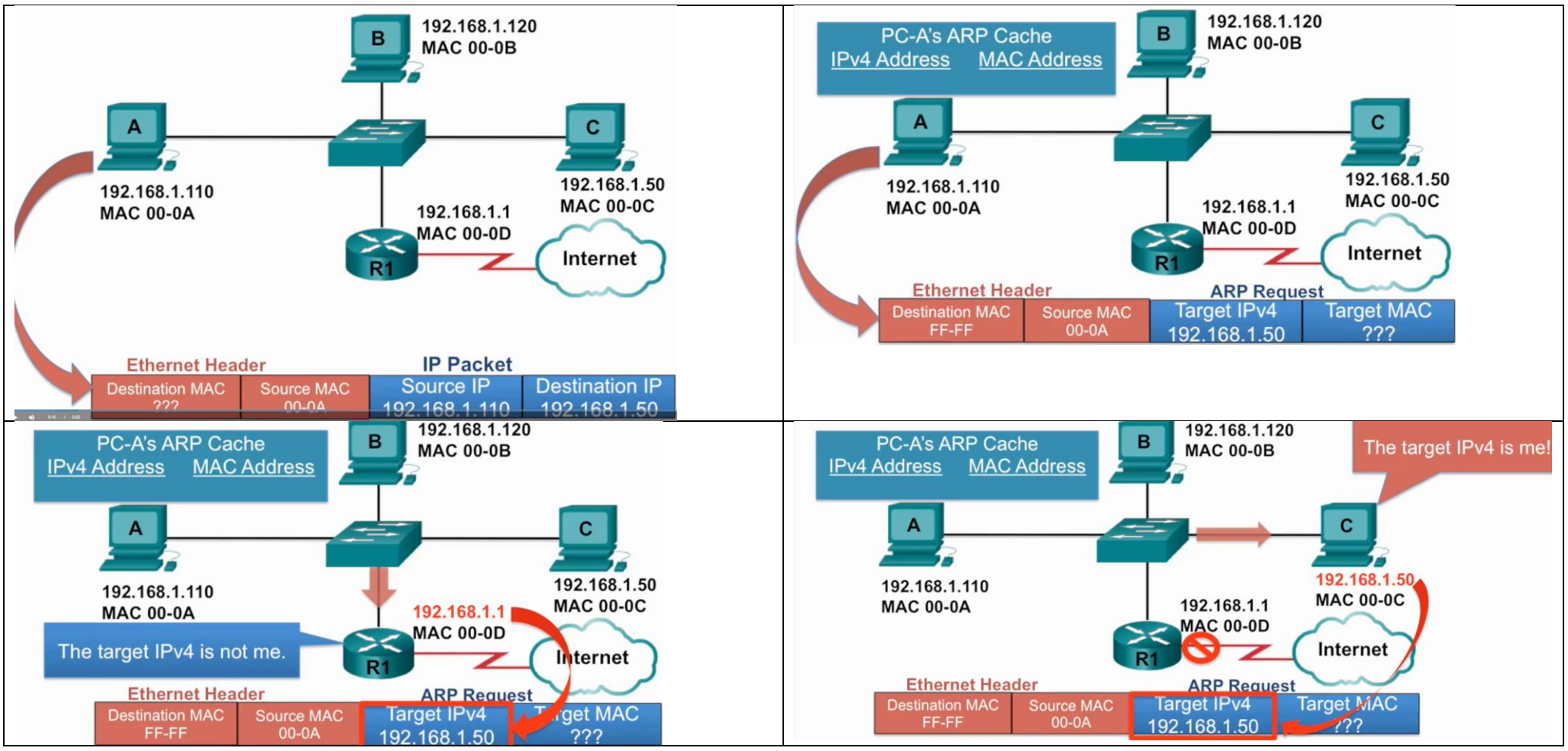
Los mensajes de ARP se encapsulan dentro de una trama *(frame)* de Ethernet, no utilizan encabezado de IPv4. La solicitud de ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:

- **Dirección MAC de destino** – Esta es una dirección ***broadcast*** que requiere a todas las NIC Ethernet de la LAN para que acepten y procesen la solicitud de ARP.
- **Dirección MAC de origen** – Esta es la dirección MAC del remitente de la solicitud ARP.
- **Tipo** - Los mensajes de ARP tienen un campo de tipo **0x806**. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.

Como las solicitudes ARP son ***broadcast***, el switch las envía por todos los puertos, excepto el de recepción. Todas las NIC Ethernet de la LAN procesan transmisiones y deben entregar la solicitud ARP a su sistema operativo para su procesamiento. Cada dispositivo procesa la solicitud ARP para ver si la dirección IPv4 objetivo coincide con la suya. Ojo que un router no reenvía difusiones por otras interfaces.

Solo un dispositivo de la LAN tiene el IPv4 que coincide con el IPv4 objetivo de la solicitud ARP. Los demás dispositivos no envían una respuesta.

En este video, vamos a ver a PCA enviar una solicitud ARP para encontrar la dirección Mac de PCC. PCA tiene un paquete IP con su IP de origen 192.168.1.110 y la IP de destino de PCC que es 192.168.1.50, están en la misma red, pero se necesita saber la MAC de destino. La PCA verifica su cache ARP y comprueba que no se encuentra la MAC de destino, pone el paquete en espera y crea una solicitud ARP. La solicitud ARP contendrá la dirección IPv4 de destino que PCA conoce, lo que se desconoce es la dirección Mac de destino, eso es lo que PCA quiere averiguar. La solicitud ARP se envía como una transmisión, por lo que todos en la red examinan la trama Ethernet y procesan la solicitud ARP. PCA la envía al conmutador porque es una transmisión, el conmutador inundará todos los puertos excepto el puerto en el que entró. La PCB recibe la transmisión, la procesa, compara su propia IPv4 con la dirección IPv4 de destino de la trama, y nota que no coinciden, no enviará una respuesta ARP. El enrutador también recibe la ARP REQUEST, su proceso ARP examina su propia IPv4 y la compara con la IPv4 de destino, también se da cuenta de que no es su dirección IPv4, no enviará la respuesta ARP. Por cierto, los enrutadores no reenvían una solicitud ARP a sus otros puertos. La PCC recibe la solicitud ARP, compara su IPv4 con la IPv4 destino y nota que es el objetivo de la solicitud ARP, que la dirección IPv4 objetivo coincide con su propio IPv4, por lo tanto, la PCC deberá enviar una respuesta ARP con su propia dirección MAC, la que se necesitaba saber.



7.1.4 Vídeo - Operación de ARP - Respuesta de ARP

Solo el dispositivo con la dirección IPv4 de destino asociada con la solicitud ARP responderá con una respuesta ARP. La ***respuesta ARP*** se encapsula en una trama de Ethernet con la siguiente información de encabezado:

- **Dirección MAC de destino** – Es la dirección MAC del remitente de la solicitud de ARP.
- **Dirección MAC de origen** – Esta es la dirección MAC del remitente de la respuesta ARP.
- **Tipo** - Los mensajes de ARP tienen un campo de tipo 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.

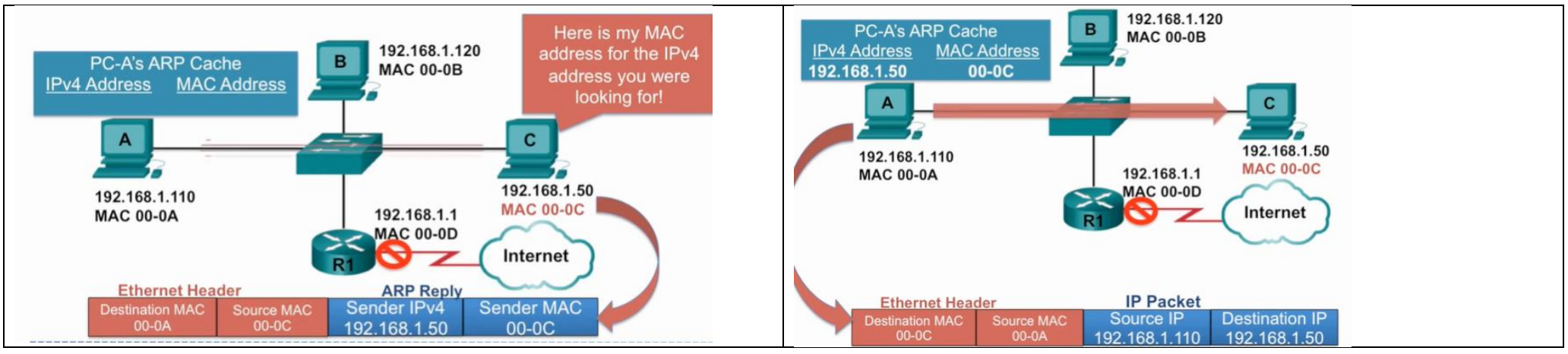
Solo el dispositivo que envió la solicitud ARP recibe una respuesta unidifusión ARP, agrega la IPv4 y la MAC correspondiente a su tabla ARP. A partir de ese momento, los paquetes destinados para esa dirección IPv4 se pueden encapsular en las tramas con la dirección MAC correspondiente. Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no se puede crear una trama.

Las entradas de la tabla ARP tienen marcas de tiempo. Si un dispositivo no recibe una trama de un dispositivo en particular antes de que caduque la marca de tiempo, la entrada para este dispositivo se elimina de la tabla ARP.

Además, se pueden introducir entradas estáticas de asignaciones en una tabla ARP, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP no caducan con el tiempo y se deben eliminar de forma manual.

Nota: IPv6 utiliza un proceso similar al ARP para IPv4, llamado "***detección de vecinos (ND) ICMPv6***". El protocolo IPv6 utiliza mensajes de ***solicitud de vecino*** y de ***anuncio de vecino*** similares a las solicitudes y respuestas ARP de IPv4.

En el video anterior vimos una solicitud ARP desde PCA buscando la dirección Mac de la PCC. En este video, veremos la respuesta ARP a esa solicitud. PCC al recibir la solicitud ARP, examino la dirección IPv4 de destino, la comparó con su propia dirección IPv4 y notó que era el objetivo previsto. Entonces, la PCC genera una ***respuesta ARP*** a esa solicitud. La respuesta ARP incluye su propia dirección IPv4 y su propia dirección MAC. La respuesta ARP se envía a PCA como unidifusión, la MAC de destino es la de PCA. PCA recibe la respuesta ARP, toma la información que contiene, esto es la dirección IPv4 del remitente, la dirección MAC del remitente y agrega esa información a su caché (memoria temporal) ARP. PCA ahora recupera el paquete original (que estuvo en espera) destinado a PCC, y ya tiene la información necesaria para enviar ese paquete a PCC. Así que toma la información de su caché ARP, la dirección MAC de PCC, y lo agrega al encabezado Ethernet como dirección de destino. PCA ahora puede reenviar este paquete en la trama Ethernet adecuada a PCC.



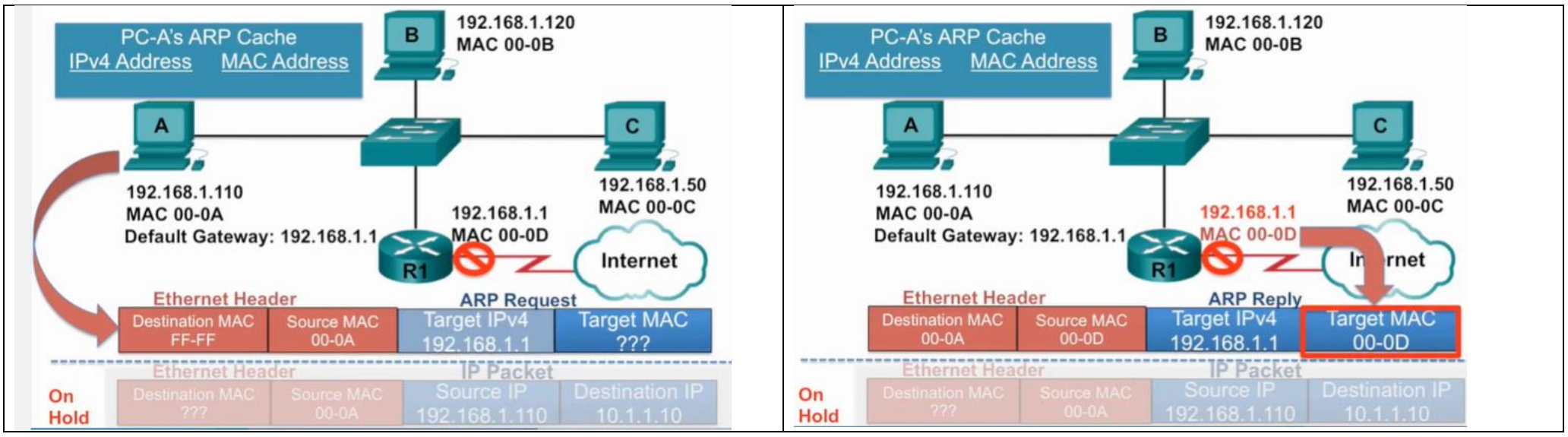
7.1.5 Video - El Rol de ARP en Comunicaciones Remotas

Cuando la dirección IPv4 de destino no está en la misma red que la dirección IPv4 de origen, el dispositivo de origen debe enviar la trama al gateway predeterminado, es decir a la interfaz del router local. Cuando un dispositivo de origen tiene un paquete con una dirección IPv4 de otra red, lo encapsula en una trama con la dirección MAC de destino del router.

La dirección IPv4 de la puerta de enlace predeterminada se almacena en la configuración IPv4 de los hosts. Cuando un host crea un paquete para un destino, compara la dirección IPv4 de destino con la propia para determinar si ambas están ubicadas en la misma red de capa 3. Si el

host de destino no está en la misma red, el origen busca en la tabla ARP la entrada que contenga la dirección IPv4 del gateway predeterminado. Si no existe, utiliza el proceso ARP para determinar la dirección MAC del gateway predeterminado.

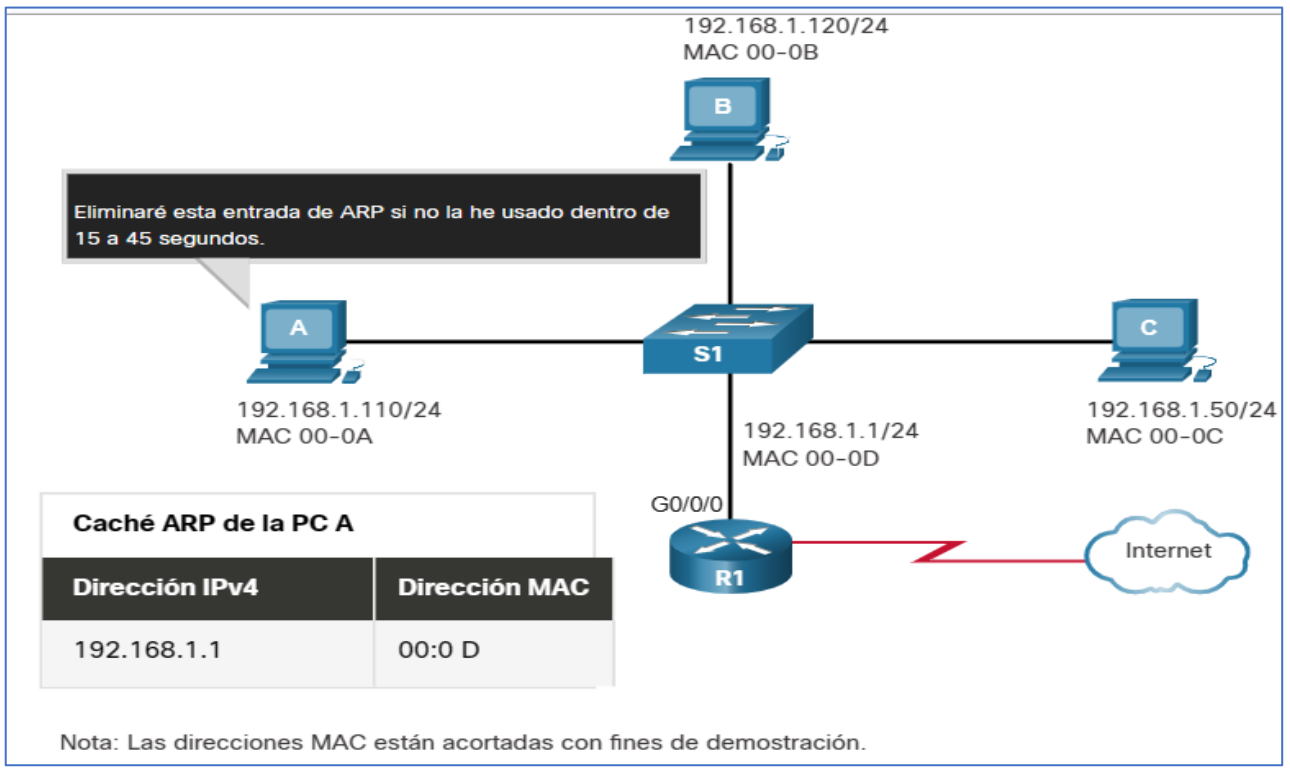
En este video, PCA tiene un paquete IP. La dirección IP de origen es 192.168.1.110 y la dirección IP de destino 10.1.1.10, es una dirección IP en una red remota. Por lo tanto, la dirección MAC de destino será la de su puerta de enlace predeterminada 192.1681.1, el enrutador R1 en este caso. PCA verifica su caché ARP para esa dirección IP 192.168.1.1 y no hay ninguna entrada con una dirección MAC, pone el paquete en espera y crea una solicitud ARP. La solicitud ARP tiene la dirección IP del enrutador 192.168.1.1, la dirección Mac de destino es desconocida. La dirección MAC de destino de una solicitud ARP es una *transmisión*, se envía al conmutador, el que inundará todos sus puertos excepto el puerto entrante. PCB recibe la solicitud ARP, compara su propia IPv4 con la IPv4 objetivo en la solicitud ARP y no coincide, no es el objetivo previsto. PCC recibe la solicitud ARP, compara su IPv4 contra la dirección de destino IPv4, y no es el objetivo tampoco. Router 1 recibe la solicitud ARP, compara su dirección IPv4 con la dirección objetivo IPv4, y de hecho es una coincidencia. Es el destino de la solicitud ARP. Por lo tanto, R1 emitirá una respuesta ARP que incluye su propia dirección MAC 000D junto a su dirección IPv4. La dirección MAC 000A de destino del ARP Reply es unicast dirigido a PCA. PCA recibe la respuesta ARP, ve la dirección IPv4 y la dirección MAC de R1 y las agrega a su caché ARP. Ahora tiene la información que necesita para reenviar el paquete que está en espera. La MAC de destino ahora será 000D, la del enrutador R1. PCA puede reenviar ahora la trama al enrutador R1.



7.1.6 Eliminando Entradas de una Tabla de ARP

Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas de ARP que no se hayan utilizado durante un período especificado. Los tiempos varían según el sistema operativo del dispositivo. Por ejemplo, los sistemas operativos Windows más recientes almacenan entradas de tabla ARP entre 15 y 45 segundos, como se ilustra en la figura.

Los comandos también se pueden usar para eliminar manualmente algunas o todas las entradas de la tabla de ARP. Después de eliminar una entrada, el proceso de envío de una solicitud de ARP y de recepción de una respuesta de ARP debe ocurrir nuevamente para que se introduzca la asignación en la tabla ARP.



7.1.7 Tablas de ARP en Dispositivos

En un enrutador Cisco, se utiliza el comando show ip arp para visualizar la tabla de ARP, como se muestra en la figura.

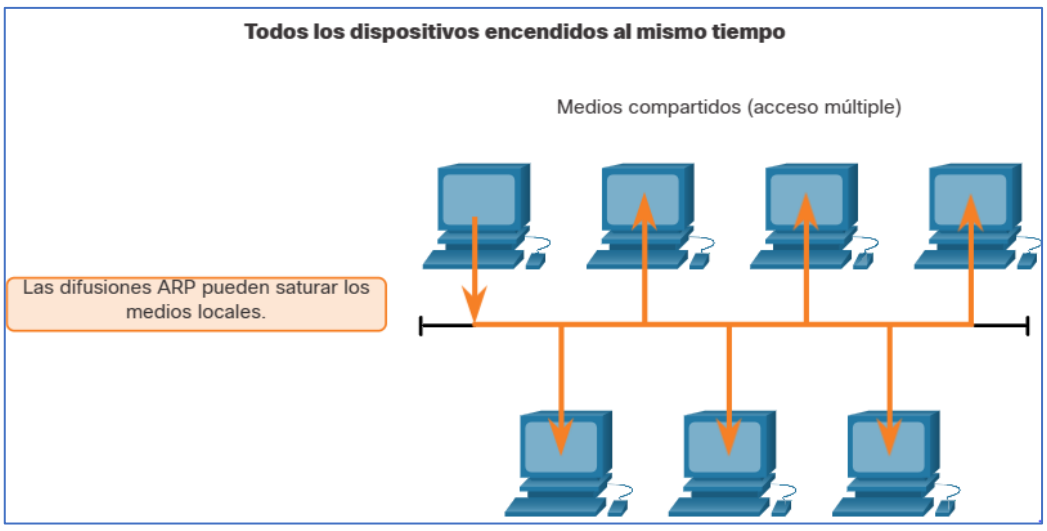
```
R1# show ip arp
Protocol   Address          Age (min)  Hardware Addr   Type  Interface
Internet   192.168.10.1            -   a0e0.af0d.e140  ARPA  GigabitEthernet0/0/0
Internet   209.165.200.225         -   a0e0.af0d.e141  ARPA  GigabitEthernet0/0/1
Internet   209.165.200.226         1   a03d.6fe1.9d91  ARPA  GigabitEthernet0/0/1
R1#
```

En una PC con Windows 10, el comando arp -a se usa para mostrar la tabla ARP, como se muestra en la figura.

```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
Internet Address      Physical Address      Type
192.168.1.1           c8-d7-19-cc-a0-86     dynamic
192.168.1.101         08-3e-0c-f5-f7-77     dynamic
192.168.1.110         08-3e-0c-f5-f7-56     dynamic
192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
192.168.1.126         24-77-03-45-5d-c4     dynamic
192.168.1.146         94-57-a5-0c-5b-02     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

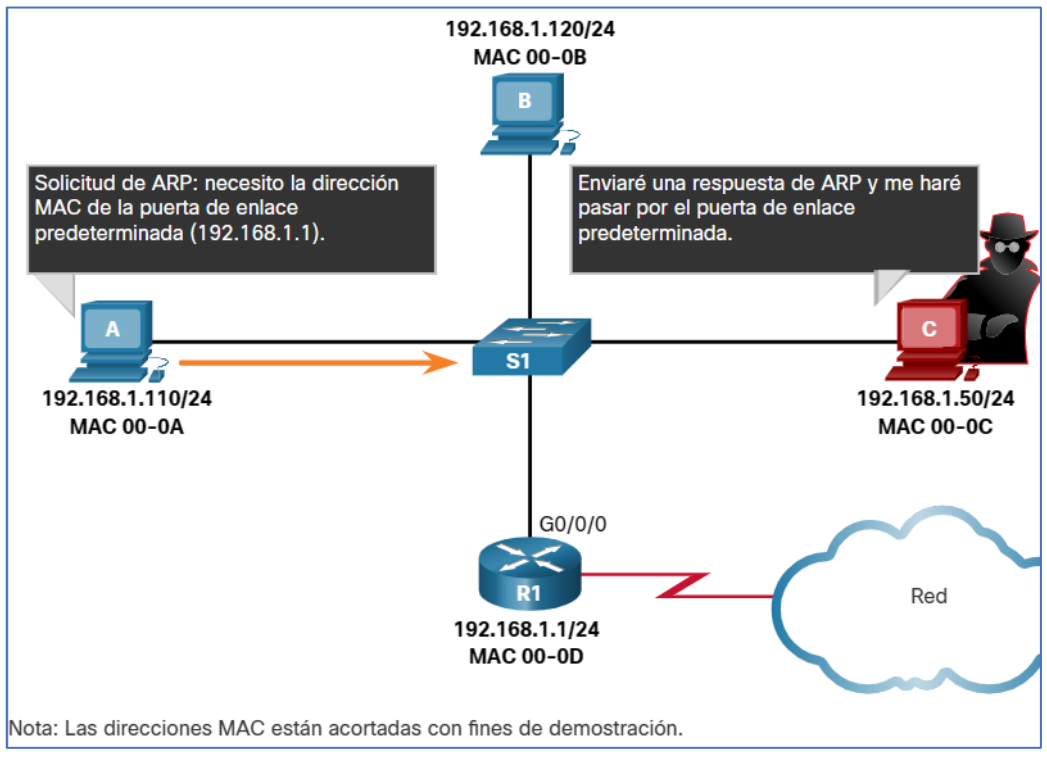
7.1.8 Problemas de ARP - Difusiones de ARP y Suplantación de Identidad de ARP

Todos los dispositivos de la red local reciben y procesan una solicitud ARP debido a que es una trama de difusión. En una red comercial típica, estas difusiones tendrían, probablemente, un efecto mínimo en el rendimiento de la red. Sin embargo, si se encendiera una gran cantidad de dispositivos que comenzaran a acceder a los servicios de red al mismo tiempo, el rendimiento podría disminuir durante un breve período, como se muestra en la figura. Después que los dispositivos envían las solicitudes de difusión ARP iniciales y obtienen las direcciones MAC necesarias, se minimiza cualquier efecto en la red.



En algunos casos, el uso de ARP puede conducir a un riesgo potencial de seguridad. Un atacante puede usar suplantación ARP para realizar un ataque de envenenamiento ARP. Esta es una técnica utilizada por un atacante cuando responde a una solicitud ARP de una dirección IPv4 que pertenece a otro dispositivo, como la puerta de enlace predeterminada, tal como se muestra en la ilustración. El atacante envía una respuesta ARP con su propia dirección MAC. El receptor de la respuesta de ARP agrega la dirección MAC incorrecta a la tabla ARP y envía estos paquetes al atacante.

Los switches de nivel empresarial incluyen técnicas de mitigación conocidas como “inspección dinámica de ARP (DAI)”. DAI está más allá del alcance de este curso.



7.1.9 Packet Tracer - Examinar la Tabla de ARP

En esta actividad de Packet Tracer, completará los siguientes objetivos:

- Examinar una Solicitud de ARP
- Examinar una tabla de direcciones MAC del switch
- Examinar el proceso ARP en comunicaciones remotas

Esta actividad está optimizada para la visualización de PDU. Los dispositivos ya están configurados. Reunirá información de PDU en el modo de simulación y responderá una serie de preguntas sobre los datos que obtenga.

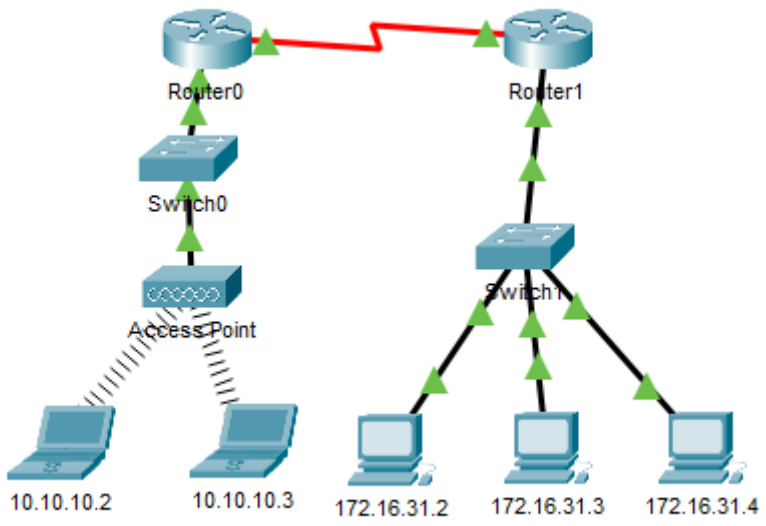


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección MAC	Interfaz del switch
Router0	Gg0/0	0001.6458.2501	G0/1
	S0/0/0	No corresponde	No corresponde
Router1	G0/0	00E0.F7B1.8901	G0/1
	S0/0/0	No corresponde	No corresponde
10.10.10.2	Inalámbrica	0060.2F84.4AB6	F0/2
10.10.10.3	Inalámbrica	0060.4706.572B	F0/2
172.16.31.2	F0	000C.85CC.1DA7	F0/1
172.16.31.3	F0	0060.7036.2849	F0/2
172.16.31.4	G0	0002.1640.8D75	F0/3

Instrucciones

Parte 1: Examinar una solicitud de ARP

Paso 1: Generar solicitudes de ARP haciendo ping a 172.16.31.3 en 172.16.31.2. Abra un símbolo del sistema.

a. Haga click en 172.16.31.2 y abra el Command Prompt.
b. Introduzca el comando arp -d para borrar la tabla ARP. Cierre símbolo del sistema
c. Ingrese al modo Simulation (Simulación) e introduzca el comando ping 172.16.31.3. Se generan dos PDU. El comando ping no puede completar el paquete ICMP sin conocer la dirección MAC del destino. Por lo tanto, la PC envía una trama de difusión de ARP para encontrar la dirección MAC del destino.
d. Haga clic en Capture/Forward (Capturar/Adelantar) una vez. La PDU ARP se mueve al Switch1, mientras que la PDU ICMP desaparece y espera la respuesta de ARP. Abra la PDU y registre la dirección MAC de destino. Pregunta: ¿Esta dirección se indica en la tabla anterior?
e. Haga clic en Capture/Forward (Capturar/Adelantar) para mover la PDU al siguiente dispositivo. Pregunta: ¿Cuántas copias de la PDU realizó el Switch1? ¿Cuál es la dirección IP del dispositivo que aceptó la PDU?
f. Abra la PDU y examine la capa 2. Pregunta: ¿Qué sucedió con las direcciones MAC de origen y destino?
g. Haga clic en Capture/Forward (Capturar/Adelantar) hasta que la PDU regrese a 172.16.31.2. Pregunta: ¿Cuántas copias de la PDU realizó el switch durante la respuesta de ARP?

Paso 2: Examinar la tabla ARP.

a. Observe que vuelve a aparecer el paquete ICMP. Abra la PDU y examine las direcciones MAC. ¿Las direcciones MAC de origen y destino coinciden con sus direcciones IP?
b. Vuelva a cambiar al modo **Realtime (Tiempo real)**; el ping se completa.
c. Haga clic en **172.16.31.2** e introduzca el comando **arp -a**. ¿A qué dirección IP corresponde la entrada de la dirección MAC? En general, ¿cuándo emite una terminal una solicitud de ARP?

Parte 2: Examinar una tabla de direcciones MAC del switch

Paso 1: Generar tráfico adicional para completar la tabla de direcciones MAC del switch. Abra un símbolo del sistema.

a. Desde 172.16.31.2, introduzca el 172.16.31.4 comando ping.
b. Haga clic en 10.10.10. 2 y abra el Command Prompt (símbolo del sistema).
c. Introduzca el comando ping 10.10.10.3. Pregunta: ¿Cuántas respuestas se enviaron y se recibieron?

Paso 2: Examinar la tabla de direcciones MAC en los switches.

a. Haga clic en **Switch1** y, a continuación, en la ficha **CLI**. Introduzca el comando **show mac-address-table**. ¿Las entradas corresponden a las de la tabla de arriba?
b. Haga clic en **Switch0** y, a continuación, en la ficha **CLI**. Introduzca el comando **show mac-address-table**. ¿Las entradas corresponden a las de la tabla de arriba? ¿Por qué hay dos direcciones MAC asociadas a un puerto?

Parte 3: Examinar el proceso ARP en comunicaciones remotas

Paso 1: Generar tráfico para producir tráfico ARP.

a. Haga click **172.16.31.2** y abra el **Command Prompt** (símbolo del sistema).

b. Introduzca el comando **ping 10.10.10.1**.

c. Escriba **arp -a**. ¿Cuál es la dirección IP de la nueva entrada de la tabla ARP?

d. Escriba **arp -d** para borrar la tabla ARP y cambiar al modo **Simulation (Simulación)**.

e. Repita el ping a 10.10.10.1. ¿Cuántas PDU aparecen?

f. Haga clic en **Capture/Forward (Capturar/Adelantar)**. Haga clic en la PDU que ahora se encuentra en el **Switch1**. ¿Cuál es la dirección IP de destino objetivo de la solicitud de ARP?

g. La dirección IP de destino no es 10.10.10.1. ¿Por qué?

Paso 2: Examinar la tabla ARP en el Router1.

a. Cambie al modo **Realtime**. Haga clic en **Router1** y, a continuación, en la ficha **CLI**.
b. Ingrese al modo EXEC privilegiado y, a continuación, introduzca el comando **show mac-address-table**. ¿Cuántas direcciones MAC figuran en la tabla? ¿Por qué?
c. Introduzca el comando **show arp**. ¿Existe una entrada para **172.16.31.2**? ¿Qué sucede con el primer ping en una situación en la que el router responde a la solicitud de ARP?

7.1.10 Laboratorio - Ver Tráfico ARP en Wireshark

En esta actividad, cumplirá los siguientes objetivos:

- Parte 1: Capturar y analizar datos de ARP en Wireshark
- Parte 2: Ver las entradas de caché ARP en la PC

Práctica de Laboratorio - Ver Tráfico ARP en Wireshark

Objetivos

Parte 1: Capturar y analizar datos de ARP en Wireshark

- Inicie y detenga la captura de datos del tráfico de ping a los hosts remotos.
- Localice la información de las direcciones IPv4 y MAC en las PDU capturadas.
- Analice el contenido de los mensajes ARP intercambiados entre los dispositivos en la LAN.

Parte 2: Ver las entradas de caché ARP en la PC

- Acceder a la línea de comandos de Windows.
- Use el comando arp de Windows para ver la caché de la tabla ARP local en la PC.

Aspectos básicos / situación

TCP/IP usa el protocolo de resolución de direcciones (ARP) para asignar una dirección IPv4 de capa 3 a una dirección MAC de capa 2. Cuando se transmite una trama Ethernet en la red, debe tener una dirección MAC de destino. Para detectar dinámicamente la dirección MAC de un destino conocido, el dispositivo de origen difunde una solicitud ARP en la red local. El dispositivo que está configurado con la dirección IPv4 de destino responde la solicitud con una respuesta ARP y la dirección MAC se registra en la caché ARP.

Cada dispositivo de la LAN mantiene su propia caché ARP. La caché ARP es un área pequeña en la RAM que conserva las respuestas ARP. Al abrir la caché ARP de una PC se puede ver la dirección IPv4 y la dirección MAC de cada dispositivo en la LAN con el que la PC ha intercambiado mensajes ARP.

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para la solución de problemas de red, análisis, desarrollo de protocolo y software y educación. Cuando los flujos de datos van y vienen por la red, el detector "captura" cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo con las especificaciones de protocolo correspondientes.

Wireshark es una herramienta útil para cualquier persona que trabaja con redes y se puede usar con la mayoría de los laboratorios en los cursos de Cisco para realizar análisis de datos y solución de problemas. Esta práctica de laboratorio proporciona instrucciones para descargar e instalar Wireshark, aunque es posible que ya esté instalado. En este laboratorio, usará Wireshark para capturar intercambios ARP en la red local.

Recursos necesarios

- 1 PC (Elección de sistema operativo con Wireshark instalado)
- Se pueden usar PC o dispositivos móviles adicionales en una red de área local (LAN) para responder a las solicitudes de ping. Si no hay dispositivos adicionales en la LAN, la dirección de la puerta de enlace predeterminada se puede usar para responder a las solicitudes de ping.

Instrucciones

Parte 1: Capturar y analizar los datos ARP locales en Wireshark

En esta parte, hará ping a otra PC en la LAN y capturará solicitudes y respuestas ARP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes para transmitir datos al destino. **Nota**: Las instrucciones están escritas para PC que ejecutan el sistema operativo Windows para su referencia.

Paso 1: Recupere las direcciones de interfaz de la PC.

Para este laboratorio, deberá conocer la dirección IPv4 y la dirección MAC de la PC. (El comando **ifconfig** para Linux y MAC OS puede proporcionar resultados similares).

a. Navegue a una ventana del Símbolo del Sistema, escriba **ipconfig /all** en el indicador.
b. Observe qué adaptador de red está usando la PC para acceder a la red. Registre la dirección IPv4 y la dirección MAC (dirección física) de la interfaz de la PC.

```
C:\Users\Student> ipconfig /all
<output omitted>
Conexión de red inalámbrica del adaptador de LAN inalámbrico:

   Connection-specific DNS Suffix. :
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
   Physical Address. . . . . . . . . : A4-AE-31-AD-78-4C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f9e7:e41d:a772:f993%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, August 04, 2016 05:35:35 PM
   Lease Expires . . . . . . . . . . : Friday, August 05, 2016 05:35:35 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 245648945
   DHCPv6 IAID . . . . . . . . . . . : 00-01-00-01-1B-87-BF-52-A4-4E-31-AD-78-4C
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

c. En la línea de comandos introduzca el comando **ipconfig**.

Registre las direcciones IPv4 de la puerta de enlace predeterminada y las otras PC de la LAN. Rpta: En este ejemplo, la puerta de enlace predeterminada es 192.168.1.1 y la dirección IPv4 para esta PC es 192.168.1.8.

- **Nota:** Si utiliza un dispositivo móvil para hacer ping a la solicitud de respuesta, busque las direcciones para encontrar la dirección IP y la dirección MAC de Wi-Fi de su dispositivo móvil.
- **Nota:** Si solo tiene un dispositivo, la dirección IP de la otra PC puede ser el gateway predeterminado.

Paso 2: Inicie Wireshark y comience a capturar datos

a. En su PC, inicie Wireshark. Nota: De manera alternativa, es posible que su instalación de Wireshark también le dé la opción Wireshark Legacy. Esto muestra Wireshark en la GUI anterior, más antigua pero bien conocida. El resto de esta práctica de laboratorio se completó con la GUI más nueva.
b. Después de que se inicie Wireshark, seleccione la interfaz de red que identificó con el comando ipconfig. Escriba arp en el cuadro del filtro. Esta selección configura Wireshark para que solo muestre los paquetes que son parte de los intercambios ARP entre los dispositivos de la red local. Haga clic con el botón derecho en la interfaz y haga clic en Iniciar Captura para comenzar la captura de datos. La información comienza a desplazar hacia abajo la sección superior de Wireshark. Cada línea representa un mensaje que se está enviando entre un dispositivo de origen y uno de destino en la red.
c. En una ventana del Símbolo del Sistema, haga ping a la puerta de enlace predeterminada para probar la conectividad con la dirección de la puerta de enlace predeterminada que se identificó en el paso anterior. (Para Linux y MAC OS, utilice el comando ping -c 4 192.168.1.1 en este ejemplo).

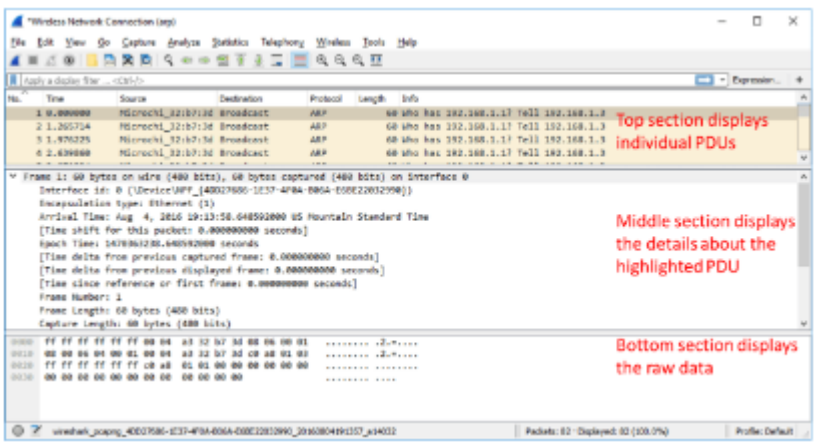
```
C:\Users\Student> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=7ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 7ms, Average = 4ms
```

d. Haga ping a las direcciones IPv4 de otras PC o dispositivos móviles en la LAN que registró en el paso anterior. **Nota:** Si su otro dispositivo no responde a sus pings, es posible que el firewall esté bloqueando estas solicitudes. Busque desbloquear el firewall para su sistema operativo en Internet.
e. Deje de capturar datos haciendo clic en Detener captura (Stop Capture) (icono de cuadrado rojo) en la barra de herramientas.

Paso 3: Examine los datos capturados

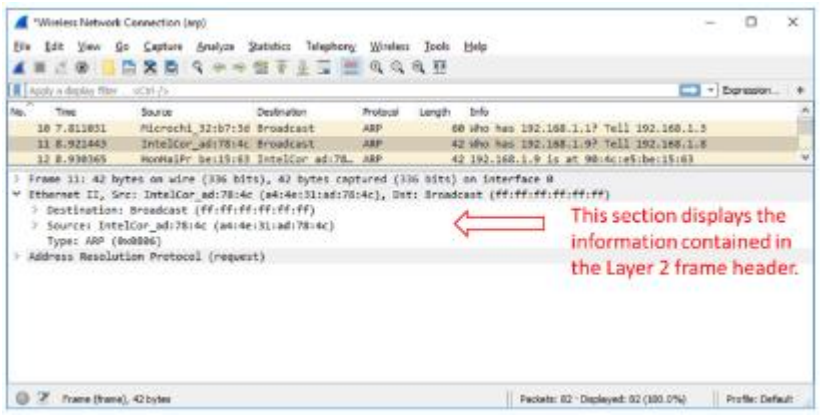
a) En este paso examinarán los datos que se generaron mediante las solicitudes de ping de la PC miembro de su equipo. Los datos de Wireshark se muestran en tres secciones:

1. La sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IPv4.
2. La sección del medio muestra la información de PDU de la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas del protocolo.
3. La sección inferior muestra los datos de cada capa sin formato. Los datos sin procesar se muestran en formatos hexadecimal y decimal.



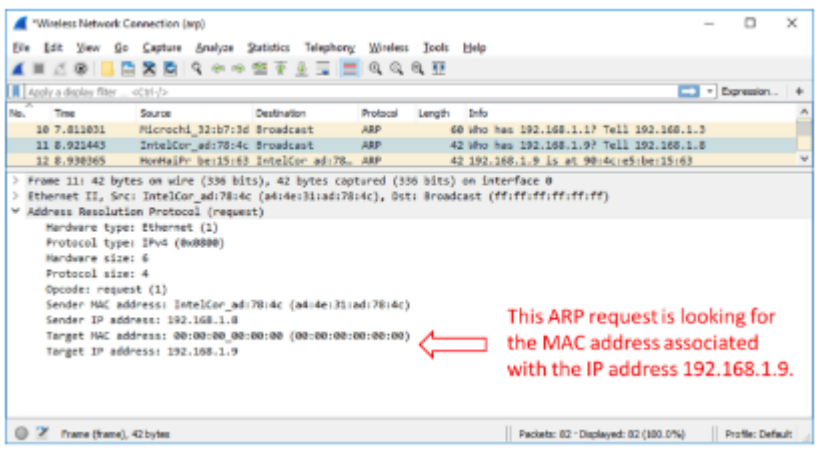
b) Haga clic en una de las tramas ARP de la parte superior que tenga la dirección MAC de la PC como dirección de origen en la trama y “difusión” como el destino de la trama.

c) Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la sección media. Haga clic en la flecha que se encuentra a la izquierda de la fila Ethernet II para ver las direcciones MAC de origen y de destino.



¿La dirección MAC de origen coincide con la interfaz de su PC? Rpta: Si.

d) Haga clic en la flecha que se encuentra a la izquierda de la fila Protocolo de resolución de direcciones (solicitud) para ver el contenido de la solicitud ARP.



Paso 4: Localice la trama de respuesta ARP que corresponde a la solicitud ARP que seleccionó.

a) Con la dirección IPv4 de destino en la solicitud ARP, localice la trama de respuesta ARP en la sección superior de la pantalla de la captura de Wireshark. Pregunta: ¿Cuál es la dirección IPv4 del dispositivo de destino de su solicitud ARP? Rpta: en nuestro ejemplo, es 192.168.1.9.

b) Seleccione la trama de respuesta en la sección superior del resultado de Wireshark. Es posible que deba desplazarse por la ventana para encontrar la trama de respuesta que coincida con la dirección IPv4 de destino identificada en el paso anterior. Amplíe las filas Ethernet II y Protocolo de resolución de direcciones (respuesta) en la sección del medio de la pantalla. Preguntas:

- ¿La trama de respuesta ARP es una trama de difusión? Rpta: No.
- ¿Cuál es la dirección MAC de destino de la trama? Rpta: la dirección MAC de destino sería a4:4e:31:ad:78:4c en este ejemplo.
- ¿Es la dirección MAC de su PC? Rpta: Si.
- ¿Qué dirección MAC es el origen de la trama? Rpta: El dispositivo que responde a la solicitud de ping.

c) Verifique que la dirección MAC coincida con la dirección MAC del dispositivo que ha seleccionado para responder a las solicitudes de ping.

Parte 2: Examine las entradas de la caché ARP en la PC.

Después de recibir la respuesta ARP en la PC, la asociación de la dirección MAC con la dirección IPv4 se almacena en la memoria caché en la PC. Estas entradas permanecerán en la memoria por un breve período (de 15 a 45 segundos); luego, si no se usan durante ese período, se borran de la caché. (Nota: busque en Internet para encontrar los comandos relacionados con ARP para una PC con sistema operativo Linux o MAC).

a. Abra una ventana de línea de comandos en la PC. En la línea de comandos ingrese arp –a y presione Enter.

```
C:\Users\Student> arp -a

Interface: 192.168.1.8 --- 0xb
  Internet Address Physical Address Type
  192.168.1.1 00-37-73-ea-b1-7a dynamic
  192.168.1.9 90-4c-e5-be-15-63 dynamic
  192.168.1.13 a4-4e-31-ad-78-4c dynamic
  224.0.0.5 01-00-5e-00-00-05 static
  224.0.0.6 01-00-5e-00-00-06 static
  224.0.0.22 01-00-5e-00-00-16 static
  224.0.0.252 01-00-5e-00-00-fc static
  224.0.0.253 01-00-5e-00-00-fd static
  239.255.255.250 01-00-5e-7f-ff-fa static
  255.255.255.255 ff-ff-ff-ff-ff-ff static
```

La salida del comando arp –a muestra las entradas que están en el caché de la PC. En el ejemplo, la PC tiene entradas para el gateway predeterminado (192.168.1.1) y para dos PC que se encuentran en la misma LAN (192.168.1.9 y 192.168.1.13).

Pregunta: ¿Cuál es el resultado de ejecutar el comando arp – a en tu PC? Rpta: El comando enumera los enlaces de direcciones MAC a IPv4 conocidos.

b) El comando arp en la PC con Windows tiene otra función. Introduzca arp /? en el símbolo del sistema y presione enter. Las opciones del comando arp le permiten ver, agregar y eliminar entradas de la tabla ARP si es necesario. Pregunta: ¿Qué opción elimina una entrada de la caché ARP? Rpta: arp -d

c) ¿Cuál sería el resultado de emitir el comando arp –d *? Rpta: Eliminaría las asignaciones de direcciones actuales en la caché ARP. Este comando requiere privilegios administrativos en Windows 10.

Reflexión

1. ¿Cuál es el beneficio de mantener las entradas de la caché ARP en memoria en la computadora de origen? Rpta: Su computadora revisa siempre su caché local antes de solicitar información de otros dispositivos en la red. La caché ARP retiene las asociaciones de direcciones

obtenidas dinámicamente correspondientes a un período breve. Cuando se intercambia tráfico a menudo entre el origen y el destino, la caché ARP evita que el host difunda solicitudes ARP innecesariamente.

2. Si la dirección IPv4 de destino no se encuentra en la misma red que el host de origen, ¿qué dirección MAC se usará como dirección MAC de destino en la trama? Rpta: La computadora usará la dirección MAC de la puerta de enlace predeterminada.

7.1.11 Verifique su Comprensión – ARP

¿Qué dos funciones proporciona ARP? (Elija dos opciones).

Mantiene una tabla de direcciones IPv4 a los nombres de dominio	Mantiene una tabla de asignaciones de direcciones IPv4 a MAC ☺←
Mantiene una tabla de asignaciones de direcciones IPv6 a MAC	Resuelve direcciones IPv4 a nombres de dominio
Resuelve direcciones IPv4 a direcciones MAC ☺←	Resuelve direcciones IPv6 a direcciones MAC

ARP tiene dos funciones principales: mantener una tabla de asignaciones de direcciones IPv4 a MAC y determinar las direcciones MAC de direcciones IPv4 conocidas.

¿Dónde se almacena la tabla ARP en un dispositivo?

ROM	Memoria flash	NVRAM	RAM ☺←

La tabla ARP se almacena en caché temporalmente en la RAM.

¿Qué afirmación es verdadera sobre ARP?

No se puede eliminar manualmente una memoria caché ARP.	Las entradas ARP se almacenan en caché de forma permanente.	Las entradas ARP se almacenan en caché temporalmente. ☺←

¿Qué comando se podría usar en un router Cisco para ver su tabla ARP?

arp -a	arp -d	show arp table	show ip arp ☺←

¿Qué es un ataque usando ARP?

broadcasts ARP	ataques ARP hopping	ARP poisoning ☺←	ARP starvation

La suplantación de envenenamiento ARP consiste en infectar un dispositivo conectado a una red, con el fin de que este le haga creer a los otros ordenadores que él es el router. Esto se logra cambiando la dirección física de la tarjeta de red original por la dirección MAC del atacante.

2. Resumen de Resolución de Direcciones

7.2.1 ¿Qué Aprendí en este Módulo?

ARP

Para enviar un paquete a otro host en la misma red IPv4 local, un host debe conocer la dirección IPv4 y la dirección MAC del dispositivo de destino. Las direcciones IPv4 de destino del dispositivo se conocen o se resuelven por el nombre del dispositivo. Sin embargo, las direcciones MAC deben ser descubiertas. Un dispositivo utiliza el protocolo ARP para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4. ARP proporciona dos funciones básicas: resolver direcciones IPv4 a direcciones MAC y mantener una tabla de asignaciones de direcciones IPv4 a MAC.

El dispositivo emisor busca en su tabla ARP la dirección IPv4 de destino y la dirección MAC correspondiente.

- Si la dirección IPv4 de destino del paquete está en la misma red que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 de destino en la tabla ARP.
- Si la dirección IPv4 de destino está en una red diferente que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 del gateway predeterminado.

En cada entrada o fila de la tabla ARP, se enlaza una dirección IPv4 con una dirección MAC. La relación entre los dos valores se denomina asignación. Los mensajes ARP se encapsulan directamente dentro de una trama Ethernet. No se utiliza un encabezado de IPv4. La solicitud de ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:

- Dirección MAC de destino – Una dirección *broadcast*. Requiere que todas las NIC Ethernet de la LAN acepten y procesen la solicitud ARP.
- Dirección MAC de origen – La dirección MAC del remitente de la solicitud ARP.
- Tipo - Los mensajes de ARP tienen un campo de tipo 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.

Como las solicitudes de ARP son de *broadcast,* el switch las envía por todos los puertos, excepto el de recepción. Sólo el dispositivo con la dirección IPv4 de destino asociada con la solicitud ARP responderá con una respuesta ARP. Una vez que recibe la respuesta ARP, el dispositivo agrega la dirección IPv4 y la dirección MAC correspondiente a su tabla ARP.

Cuando la dirección IPv4 de destino no está en la misma red que la dirección IPv4 de origen, el dispositivo de origen debe enviar la trama al gateway predeterminado, es decir a la interfaz del router local. Cuando un dispositivo de origen tiene un paquete con una dirección IPv4 de otra red, lo encapsula en una trama con la dirección MAC de destino del router. La dirección IPv4 de la puerta de enlace predeterminada se almacena en la configuración IPv4 de los hosts. Si el host de destino no está en la misma red, el origen busca en la tabla ARP una entrada que contenga la dirección IPv4 del gateway predeterminado. Si no existe una entrada, utiliza el proceso ARP para determinar la dirección MAC del gateway predeterminado.

Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas de ARP que no se hayan utilizado durante un período especificado. Los tiempos varían según el sistema operativo del dispositivo. Los comandos se pueden usar para eliminar manualmente algunas o todas las entradas de la tabla de ARP.

En un router Cisco, se utiliza el comando ***show ip arp*** para visualizar la tabla de ARP. En una PC con Windows 10, se utiliza el comando ***arp –a*** para visualizar la tabla de ARP.

Todos los dispositivos de la red local reciben y procesan una solicitud de ARP debido a que es una trama de difusión. Si se encendiera una gran cantidad de dispositivos que comenzaran a acceder a los servicios de red al mismo tiempo, el rendimiento podría disminuir durante un breve período de tiempo. En algunos casos, el uso de ARP puede conducir a un riesgo potencial de seguridad.

Un atacante puede usar suplantación ARP para realizar un ataque de envenenamiento ARP. Esta es una técnica utilizada por un actor de amenazas para responder a una solicitud ARP de una dirección IPv4 que pertenece a otro dispositivo, como la puerta de enlace predeterminada. El atacante envía una respuesta de ARP con su propia dirección MAC. El receptor de la respuesta de ARP agrega la dirección MAC incorrecta a la tabla ARP y envía estos paquetes al atacante.

7.2.2 Webster - Preguntas de Reflexión

Olcay y Abay saben mucho sobre redes, incluida la resolución de direcciones. Antes de este módulo, ¿entendía ARP y las tablas de ARP? ¡Nunca había pensado en un actor de amenazas que usara la suplantación de identidad ARP para realizar un ataque de envenenamiento ARP! ¿Y tú?

7.2.3 Prueba de Resolución de Direcciones

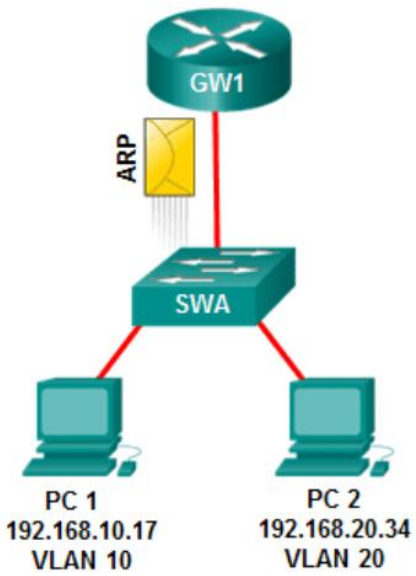
¿Qué protocolo se utiliza para detectar la dirección de destino que se debe agregar a una trama de Ethernet?

ARP ☺←	DNS	DHCP	HTTP

¿Cuál es la función del protocolo ARP?

obtener una dirección IP automáticamente	mapear un nombre de dominio a su dirección IP
resolver una dirección IPv4 a una dirección MAC ☺←	mantener una tabla de nombres de dominio con sus direcciones IP resueltas

Consultar la ilustración. La PC1 en la VLAN 10 desea comunicarse con la PC2 en la VLAN 20. PC1 envía una solicitud ARP a su puerta de enlace predeterminada, GW1. ¿Cómo responde GW1?



Envía una respuesta ARP a la PC2.	Envía una solicitud ARP a la PC1.
Reenvía la solicitud ARP de PC1 a PC2.	Envía una respuesta ARP a PC1 con su propia dirección MAC. ☺←

¿Qué acción toma el proceso ARP cuando un host necesita construir una trama, pero el caché ARP no contiene un mapeo de direcciones?

El proceso ARP envía una solicitud ARP a la dirección de difusión Ethernet para detectar la dirección IPv4 del dispositivo de destino.
El proceso ARP envía una solicitud ARP a la dirección de difusión IPv4 para detectar la dirección MAC del dispositivo de destino.
El proceso ARP envía una solicitud ARP a la dirección de difusión IPv4 para detectar la dirección IPv4 del dispositivo de destino.
El proceso ARP envía una solicitud ARP a la dirección de difusión Ethernet para detectar la dirección MAC del dispositivo de destino. ☺←

¿Cuál de las siguientes afirmaciones describe el tratamiento de las solicitudes ARP en el enlace local?

Deben reenviarlas todos los routers de la red local.	Las reciben y las procesan todos los dispositivos de la red local. ☺←
Las descartan todos los switches de la red local.	Las recibe y las procesa solamente el dispositivo objetivo.

¿Cuál es el objetivo de un ataque de suplantación de ARP?

Inundar la red con transmisiones de respuesta de ARP	Llenar las tablas de direcciones MAC del switch con direcciones falsas.
Asociar direcciones IP con direcciones MAC incorrectas. ☺←	Abrumar a los hosts de la red con solicitudes ARP.

Un analista especializado en ciberseguridad cree que un atacante está anunciando una dirección MAC falsificada a hosts de red para falsificar el gateway predeterminado ¿Qué comando puede utilizar el analista en los hosts de red para ver qué dirección MAC utilizan los hosts para llegar al gateway predeterminado?

netstat -r	route print	ipconfig /all	arp -a ☺←

¿Qué hará primero un host al preparar una PDU de capa 2 para su transmisión a un host en la misma red Ethernet?

Enviará la PDU al router conectado directamente a la red.	Se consultará en el servidor DNS local el nombre del host de destino.
Buscará en la tabla ARP la dirección MAC del host de destino. ☺←	Iniciará una solicitud ARP para encontrar la dirección MAC del host de destino.

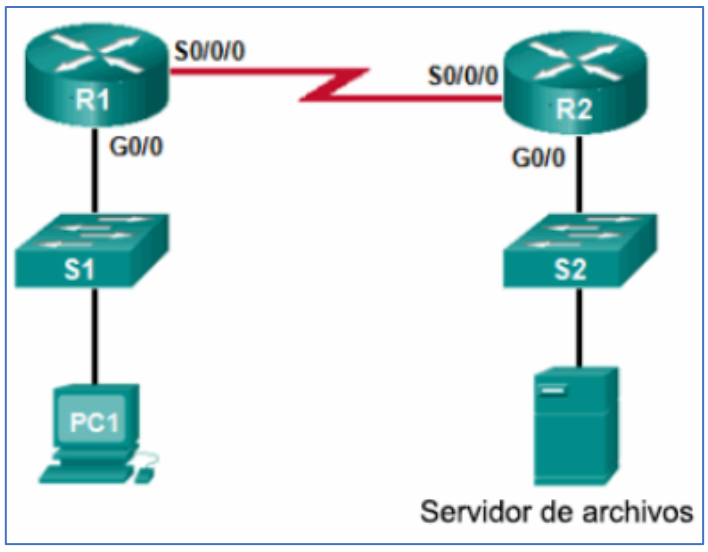
¿Qué dirección de destino se utiliza en una trama de solicitud ARP?

0.0.0.0	255.255.255.255
FFFF.FFFF.FFFF ☺←	127.0.0.1
01-00-5E-00-AA-23	

¿Qué protocolo utiliza una computadora para encontrar la dirección MAC de la puerta de enlace predeterminada en una red Ethernet?

ARP ☺←	TCP	UDP	DHCP

Consultar la ilustración. La PC1 intenta conectarse con File_server1 y envía una solicitud ARP para obtener una dirección MAC de destino. ¿Qué dirección MAC recibirá la PC1 en la respuesta ARP?



la dirección MAC de S1	la dirección MAC de la interfaz G0/0 en R1 ☺←
la dirección MAC de la interfaz G0/0 en R2	la dirección MAC de S2
la dirección MAC de File_server1	

Módulo 8: Servicios de Direccionamiento IP

0. Introducción

8.0.1 Webster - ¿Por Qué Debería Tomar este Módulo?

Hola. Mientras que Olcay y Abay trabajan juntos, Olcay debe utilizar el comando nslookup para verificar el estado actual de los servidores de nombres. Olcay aprovecha esta oportunidad para ver qué sabe Abay sobre los servicios DNS y DHCP. Abay explica que el protocolo DNS define un servicio automatizado que hace coincidir los nombres de los recursos con la dirección de red numérica requerida. También le explica sobre DHCP. En lugar de usar direccionamiento estático para cada conexión, es más eficiente tener direcciones IPv4 asignadas automáticamente usando DHCP. ¡Olcay está impresionado con el conocimiento de Abay! Realmente ha estado haciendo su tarea.

¿Puedes explicar cómo funcionan los servicios DNS y DCHP? Apuesto a que este módulo ayudará. ¡Sigue leyendo!

8.0.2 ¿Qué Aprenderé en este Módulo?

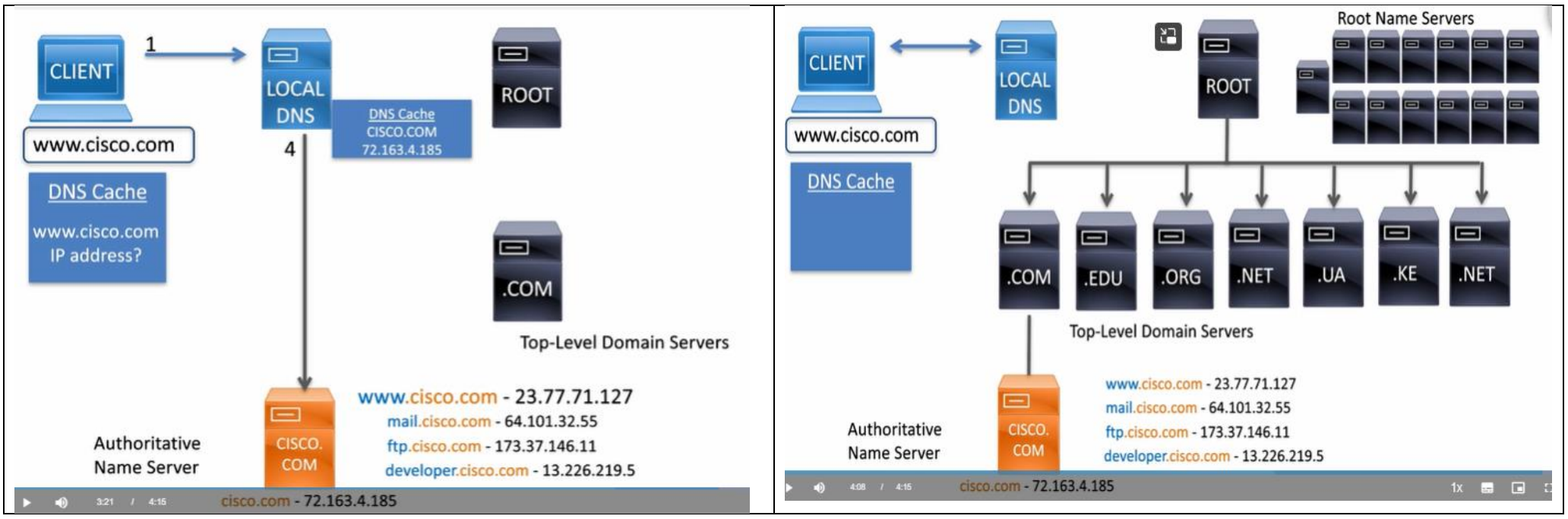
- Título del Módulo: Servicios de Direccionamiento IP
- Objetivo del Módulo: Explicar cómo funcionan los servicios DNS y DHCP

Título del Tema	Objetivo del Tema
Servicios de DNS	Explicar cómo funciona el DNS
Servicios de DHCP	Explicar cómo funciona el DHCP

1. Servicios de DNS

8.1.1 Vídeo - Sistema de Nombres de Dominio

Cuando ingresamos un nombre de dominio como la URL www.cisco.com, ¿cómo sabe nuestro cliente la dirección IP con ese nombre de dominio? La respuesta está en el DNS, el Sistema de Nombres de Dominio. El sistema operativo primero verificará en su caché local DNS para ver si ya tiene esta información, la dirección IP para www.cisco.com. Si la información no está presente en la caché DNS, el cliente enviará una consulta a la dirección IP de su servidor DNS local. El servidor DNS local verificará en su propia caché DNS la dirección IP asociada con www.cisco.com. Si ya contiene esta información, enviará una respuesta al cliente, de lo contrario, deberá obtener la respuesta para el cliente. El servidor DNS local, también conocido como servidor DNS recursivo, buscará una respuesta consultando a los servidores DNS raíz. Hay 13 servidores DNS raíz operados por 12 organizaciones diferentes, con más de 750 instancias de servidores en todo el mundo. Los servidores de nombres raíz remitirán las solicitudes a los servidores de dominio de nivel superior apropiados o **TLD**s (***Top Level Domain Servers***). Un de dominio de nivel superior o TLD es lo que sigue al punto final de un nombre de dominio como .com o .org. Hay servidores de dominio de nivel superior para cada TLD. Desde que nuestro cliente solicita la dirección IP para un nombre de dominio que termina en .com, el servidor de nombres raíz se referirá al servidor DNS local de .com, el servidor de nombres de dominio superior o servidor TLD. El servidor de nombres raíz envía la dirección IP de uno de los muchos servidores de TLD .com al servidor DNS local. El servidor DNS local ahora agregará la dirección IP del servidor TLD .com a su caché de DNS. Por lo general, el servidor DNS local ya tendrá la dirección IP del servidor TLD .com en su caché, por lo que no tiene que preguntarle primero al servidor de nombres raíz. El servidor DNS local ahora consultará al servidor TLD .com. Los servidores de dominio de nivel superior conocen las direcciones IP de los servidores autorizados. Un servidor DNS autorizado es el poseedor final de la dirección IP para el dominio que el cliente está buscando. En este ejemplo, cisco.com es el servidor autorizado para cualquier dominio que termine en cisco.com. Podría ser administrado por el propietario del dominio, como Cisco Systems, o por un tercero en nombre del propietario del dominio. La función del servidor TLD .com es dar al servidor DNS local la dirección IP del servidor autorizado de cisco.com. Finalmente estamos en el último servidor de nuestra jerarquía, el servidor autorizado. El servidor DNS local ahora tiene la dirección IP del servidor autorizado de cisco.com y envía una consulta al servidor cisco.com, solicitando la dirección IP de www.cisco.com, el nombre de dominio solicitado por el cliente. El servidor autorizado de cisco.com contiene todas las direcciones IP para cualquier dominio que termine en cisco.com, incluido www.cisco.com. El servidor autorizado .com envía la dirección IP de www.cisco.com al servidor DNS local. El servidor DNS local agrega esta información a su caché DNS y ahora tiene lo que necesita para el cliente. El servidor DNS local ahora puede responder a los clientes sus consultas por la dirección IP de www.cisco.com. El cliente agrega la dirección IP de www.cisco.com a su caché DNS y ahora tiene la dirección IP que necesita para enviar un paquete IP al servidor web www.cisco.com.Y aquí hay otro vistazo de quién participó en resolver nuestro nombre de dominio www.cisco.com en una dirección IP.



8.1.2 Sistema de Nombres de Dominio

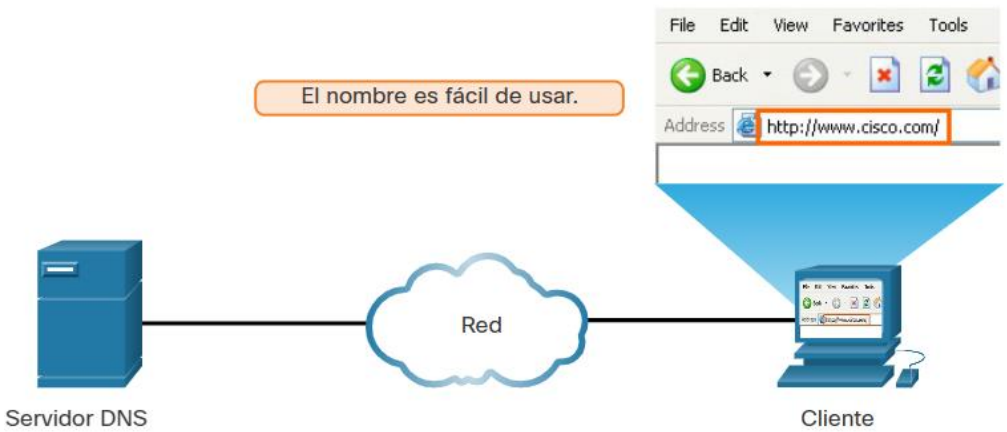
Existen otros protocolos específicos de capa de aplicación diseñados para facilitar la obtención de direcciones para dispositivos de red. Estos servicios son esenciales porque llevaría mucho tiempo recordar direcciones IP en lugar de direcciones URL o configurar manualmente todos los dispositivos de una red mediana a grande. En este tema se detallan los servicios de direccionamiento IP, DNS y DHCP.

En las redes de datos, los dispositivos se etiquetan con direcciones IP numéricas para enviar y recibir datos a través de las redes. Los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible.

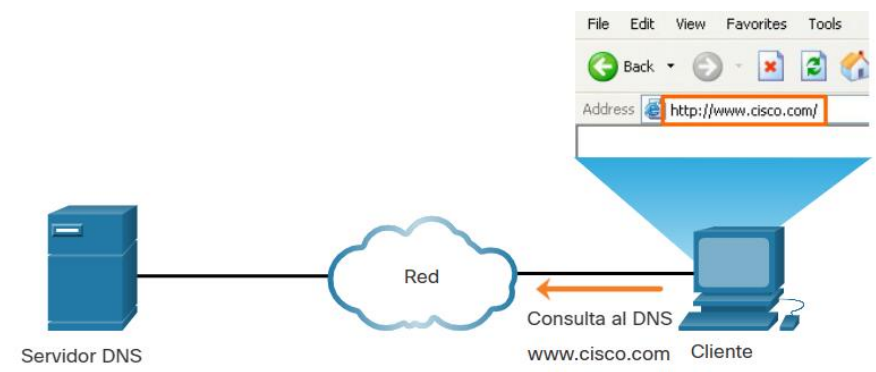
En Internet, los nombres de dominio completos (Fully Qualified Domain Name FQDN), como http://www.cisco.com, son mucho más fáciles de recordar para las personas que 198.133.219.25, que es la dirección numérica real de este servidor. Si Cisco decide cambiar la dirección numérica de www.cisco.com, esto no afecta al usuario, porque el nombre de dominio se mantiene. Simplemente se une la nueva dirección al nombre de dominio existente y se mantiene la conectividad.

El protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye el formato de consultas, respuestas y datos. Las comunicaciones del protocolo DNS utilizan un único formato llamado “mensaje”. Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

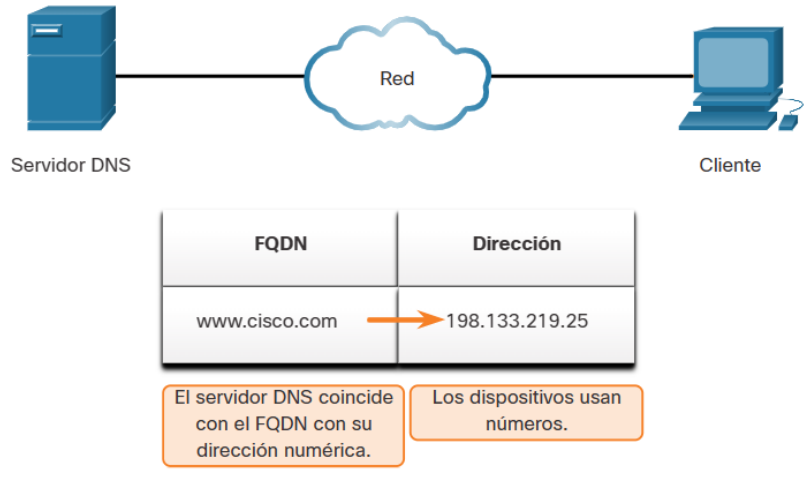
Paso 1: El usuario escribe un FQDN en un campo Dirección de aplicación del explorador.



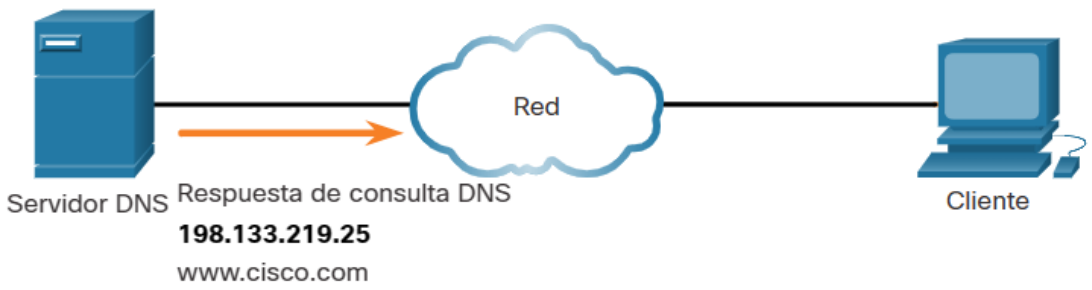
Paso 2: Se envía una consulta DNS al servidor DNS designado para el equipo cliente.



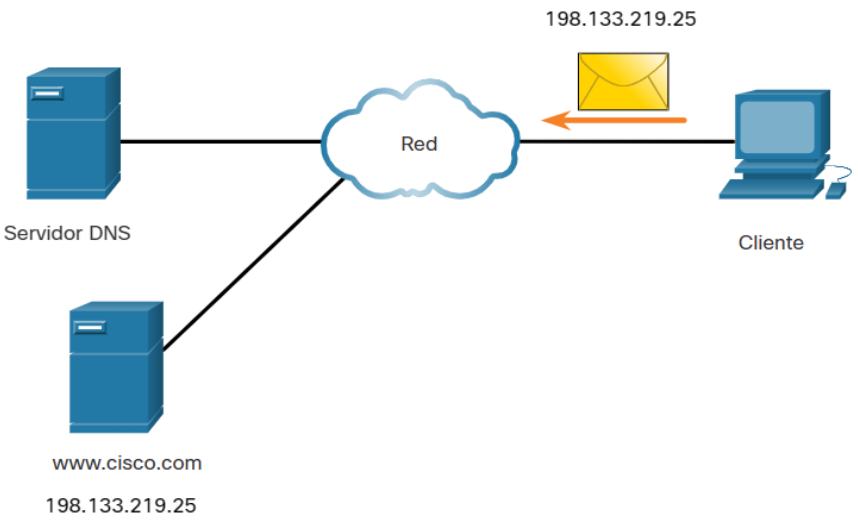
Paso 3: El servidor DNS coincide el FQDN con su dirección IP.



Paso 4: La respuesta de la consulta DNS se envía de nuevo al cliente con la dirección IP del FQDN.



Paso 5: El equipo cliente utiliza la dirección IP para realizar solicitudes del servidor.



8.1.3 Formato de Mensajes DNS

El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Estos registros contienen el nombre, la dirección y el tipo de registro. Algunos de estos tipos de registros son los siguientes:

- **A** - Una dirección IPv4 de un dispositivo final
- **NS** - Un servidor de nombre autoritativo
- **AAAA** - Una dirección IPv6 de un dispositivo final (pronunciado quad-A)
- **MX** - Un registro de intercambio de correo

Cuando un cliente realiza una consulta, el proceso DNS del servidor observa primero sus propios registros para resolver el nombre. Si no puede resolverlo con los registros almacenados, contacta a otros servidores para hacerlo. Una vez que encuentra una coincidencia se la devuelve al servidor solicitante original, este almacena temporalmente la dirección numerada por si se vuelve a solicitar el mismo nombre.

El servicio del cliente DNS en los equipos Windows también almacena los nombres resueltos previamente en la memoria. El comando ***ipconfig /displaydns*** muestra todas las entradas de DNS en caché.

Este formato de mensaje que se ve en la figura se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, para los mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Pregunta	La pregunta para el servidor de nombres
Respuesta	Registros de recursos que responden la pregunta
Autoridad	Registros de recursos que apuntan a una autoridad
Adicional	Registros de recursos que poseen información adicional

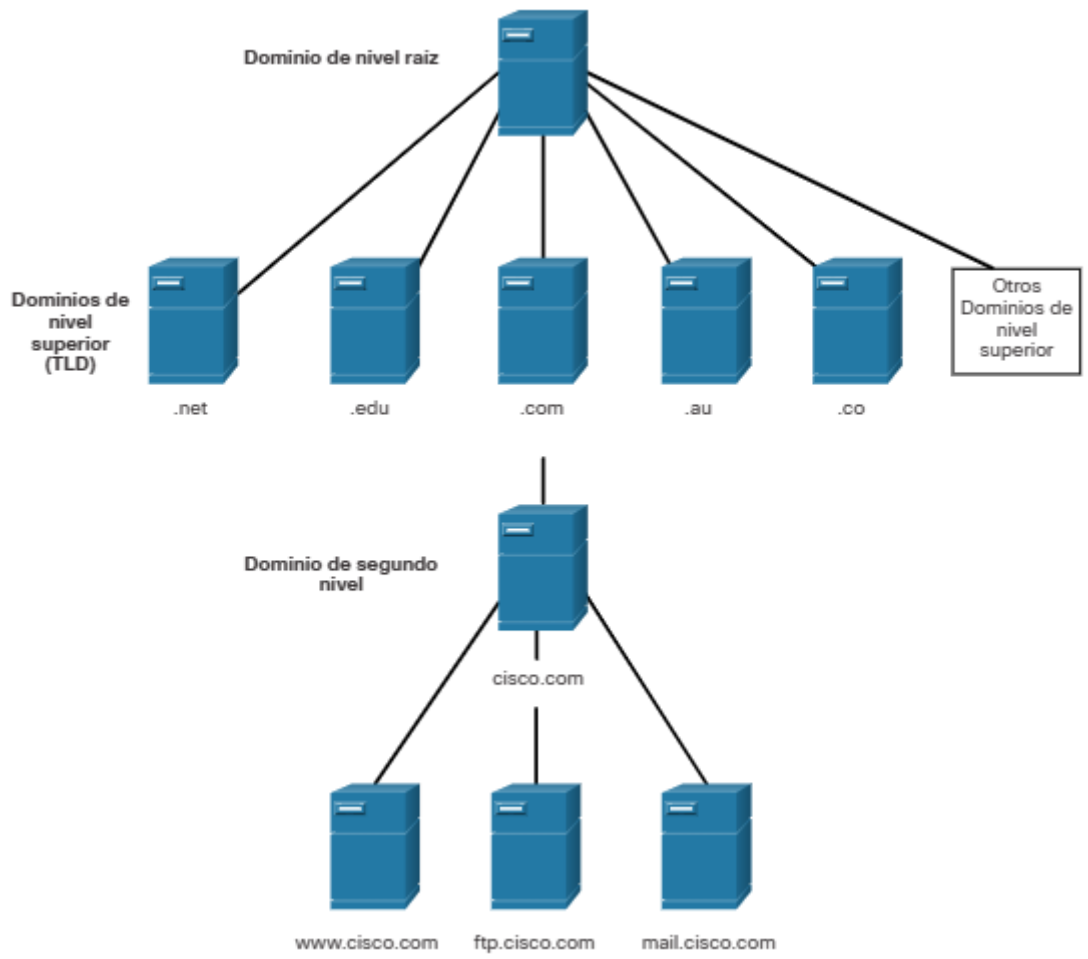
8.1.4 La Jerarquía DNS

El protocolo DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres, como se muestra en la figura. DNS utiliza nombres de domino para formar la jerarquía.

La estructura de nomenclatura se divide en zonas pequeñas y manejables. Cada servidor DNS mantiene un archivo de base de datos específico y sólo es responsable de administrar las asignaciones de nombre a IP para esa pequeña porción de toda la estructura DNS. Cuando un servidor DNS recibe una solicitud para una traducción de nombre que no se encuentra dentro de esa zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para su traducción. DNS es escalable, porque la resolución de los nombres de hosts se distribuye entre varios servidores.

Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen. Algunos ejemplos de dominios de nivel superior son los siguientes:

- **.com** - una empresa o industria
- **.org** - una organización sin fines de lucro
- **.au** – Australia
- **.co** – Colombia



8.1.5 El Comando nslookup

Al configurar un dispositivo de red, se proporcionan una o más direcciones de servidores DNS que el cliente DNS puede utilizar para la resolución de nombres. En general, el proveedor de servicios de Internet (ISP) suministra las direcciones para utilizar con los servidores DNS. Cuando la aplicación del usuario pide conectarse a un dispositivo remoto por su nombre, el cliente DNS solicitante consulta al servidor de nombres para resolver el nombre para una dirección numérica.

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:  cisco.netacad.net
Address:  72.163.6.223
>
```

Los sistemas operativos informáticos también cuentan con una herramienta llamada ***nslookup*** que permite que el usuario consulte de forma manual los servidores de nombres para resolver un nombre de host dado. Esta utilidad también puede utilizarse para solucionar los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.

En esta figura, cuando se ejecuta el comando nslookup, se muestra el servidor DNS predeterminado configurado para su host. El nombre de un host o dominio se puede ingresar en el indicador de *nslookup*. La utilidad nslookup tiene muchas opciones disponibles para realizar una prueba y una verificación exhaustivas del proceso DNS.

8.1.6 Comprobador de Sintaxis — El Comando nslookup

En el símbolo del sistema de Windows, introduzca el comando ***nslookup*** para iniciar una consulta manual de los servidores de nombres.

En los resultados aparece el nombre y la dirección IP del servidor DNS configurado en el cliente. Tenga en cuenta que la dirección del servidor DNS puede configurarse en forma manual o aprenderse dinámicamente mediante DHCP.

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2486]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\aliag>nslookup
Servidor predeterminado:  cachewas.tdp.net.pe
Address:  200.48.225.130
```

Ahora estamos en ***modo nslookup***. Ingrese www.cisco.com

En el resultado aparecen las direcciones IP relacionadas con “www.cisco.com” que el servidor “e2867” tiene actualmente en la base de datos. Observe que también se enumeran las direcciones IPv6. Además, se muestran varios alias que resolverán en “www.cisco.com”

```
> www.cisco.com
Servidor:  cachewas.tdp.net.pe
Address:  200.48.225.130

Respuesta no autoritativa:
Nombre:  e2867.dsca.akamaiedge.net
Addresses:  2600:1419:3200:181::b33
          2600:1419:3200:189::b33
          96.6.196.22
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

Introduzca el Comando exit para salir del modo nslookup y volver a la línea de comandos de Windows

```
> exit

C:\Users\aliag>
```

Puede consultar directamente los servidores DNS con solo agregar el nombre de dominio al comando nslookup.

Ingrese ***nslookup www. google.com.***

```
C:\Users\aliag>nslookup www.google.com
Servidor:  cachewas.tdp.net.pe
Address:  200.48.225.130

Respuesta no autoritativa:
Nombre:  www.google.com
Addresses:  2800:3f0:4003:c01::67
          2800:3f0:4003:c01::69
          2800:3f0:4003:c01::6a
          2800:3f0:4003:c01::93
          64.233.190.103
          64.233.190.106
          64.233.190.99
          64.233.190.104
          64.233.190.147
          64.233.190.105


C:\Users\aliag>
```

Utilizó correctamente el comando nslookup para verificar el estado de los nombres de dominio.

8.1.7 Verifique su Comprensión - Servicios de DNS

¿Cuál de los siguientes tipos de registros DNS se utiliza para resolver direcciones IPv6?

A	NS	AAAA ☺←	MN

¿Verdadero o falso? Un servidor DNS que recibe una solicitud de resolución de nombres que no está dentro de su zona DNS enviará un mensaje de error al cliente solicitante.

VERDADERO	FALSO ☺←

Cuando un servidor DNS recibe una solicitud de resolución de nombres para un nombre que no está dentro de su zona, el servidor reenviará la solicitud a otro servidor DNS.

¿Cuál de los siguientes es mostrado por la utilidad nslookup?

el servidor DNS predeterminado configurado ☺←	la dirección IP del dispositivo final	todas las entradas DNS almacenadas en caché

¿Cuál de los siguientes tipos de registros de recursos DNS resuelve los servidores de nombres autorizados?

A	NS ☺←	AAAA	MN

Los registros NS resuelven los servidores de nombres autorizados. Los registros DNS A resuelven direcciones IPv4. Los registros AAAA resuelven direcciones IPv6 y los registros MX resuelven servidores de intercambio de correo.

8.1.8 Laboratorio - Observar la Resolución de DNS

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: Observar la conversión de un URL en una dirección IP mediante DNS
- Parte 2: Observar la búsqueda DNS mediante el comando **nslookup** en un Sitio Web
- Parte 3: Observar la búsqueda DNS mediante el comando **nslookup** en Servidores de Correo

Aspectos básicos / situación

Cuando se escribe una dirección del localizador uniforme de recursos (URL), como **http://www.cisco.com**, en un navegador web, se invoca el sistema de nombres de dominio (DNS). La primera parte del URL describe el protocolo que se utiliza. Los protocolos comunes son el protocolo de transferencia de hipertexto (HTTP), el protocolo de transferencia de hipertexto sobre la capa de sockets seguros (HTTPS) y el protocolo de transferencia de archivos (FTP).

El DNS utiliza la segunda parte de la dirección URL, que en este ejemplo es www.cisco.com. DNS traduce el nombre de dominio (www.cisco.com) a una dirección IP para permitir que el host de origen llegue al servidor de destino. En esta práctica de laboratorio, observará DNS en acción y utilizará el comando **nslookup** (búsqueda de servidor de nombres) para obtener información adicional de DNS.

Recursos necesarios

1 PC (Windows con acceso a Internet y símbolo del sistema)

Instrucciones

Parte 1: Observe la conversión de un URL en una dirección IP mediante DNS

a. Abra una ventana de intérprete de comandos de Windows

b. En el símbolo del sistema, haga ping al URL de Internet Corporation for Assigned Names and Numbers (ICANN), **www.icann.org**. ICANN coordina las funciones de DNS, de las direcciones IP, de la administración del sistema de nombres de dominio superior y de la administración del sistema de servidores raíz. El equipo debe traducir www.icann.org a una dirección IP para saber adónde enviar los paquetes del protocolo de mensajes de control de Internet (ICMP).

La primera línea de la salida muestra **www.icann.org** convertido a una dirección IP por DNS. Debería poder ver el efecto del DNS, aun cuando haya un firewall instalado en la institución que impida enviar pings o aun cuando el servidor de destino haya impedido hacer ping al servidor web.

Nota: Si el nombre de dominio se resuelve en una dirección IPv6, use el comando **ping -4 www.icann.org** para traducirlo a una dirección IPv4, si lo desea.

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2486]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\aliag>ping www.icann.org

Haciendo ping a www.vip.icann.org [192.0.32.7] con 32 bytes de datos:
Respuesta desde 192.0.32.7: bytes=32 tiempo=123ms TTL=241
Respuesta desde 192.0.32.7: bytes=32 tiempo=124ms TTL=241
Respuesta desde 192.0.32.7: bytes=32 tiempo=124ms TTL=241
Respuesta desde 192.0.32.7: bytes=32 tiempo=123ms TTL=241

Estadísticas de ping para 192.0.32.7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 123ms, Máximo = 124ms, Media = 123ms

C:\Users\aliag>
```

Registre las direcciones IP de www.icann.org. Rpta: 192.0.32.7

c. Escriba las direcciones IPv4 del paso b en un navegador web, en lugar de la URL. Escriba **https://192.0.32.7** en el navegador web. Si el equipo tiene una dirección IPv6, puede introducir la dirección IPv6. **https://[2620:0:2d0:200::7]** en el navegador web.

d. Observe que la página web de inicio de ICANN se muestra sin utilizar DNS.

A la mayoría de los seres humanos nos resulta más fácil recordar palabras que números. Si le indica a alguien que acceda a **www.icann.org**, probablemente lo recordará, pero si le indica que acceda a 192.0.32.7, le resultará difícil recordar una dirección IP. Los equipos informáticos procesan números (sistema binario). El DNS es el proceso por el cual las palabras se traducen por números. Además, hay una segunda traducción que tiene lugar. Los seres humanos pensamos en números con base 10. En informática, se procesan números con base 2. La dirección IP 192.0.32.7 con base 10 es equivalente a 11000000.00000000.00100000.00000111 con base 2. ¿Qué sucede si corta estos números con base 2 y los pega en un navegador?

Rpta: *El sitio web no aparece. El código de software que se usa en los navegadores web reconoce números con base 10, no reconoce números con base 2.*

e. En el símbolo del sistema, haga ping a www.cisco.com.

Nota: Si el nombre de dominio se resuelve en una dirección IPv6, use el comando ping -4 www.cisco.com para traducirlo por una dirección IPv4, si lo desea.

```
C:\Users\aliag>ping www.cisco.com

Haciendo ping a e2867.dsca.akamaiedge.net [96.6.196.22] con 32 bytes de datos:
Respuesta desde 96.6.196.22: bytes=32 tiempo=8ms TTL=57
Respuesta desde 96.6.196.22: bytes=32 tiempo=8ms TTL=57
Respuesta desde 96.6.196.22: bytes=32 tiempo=6ms TTL=57
Respuesta desde 96.6.196.22: bytes=32 tiempo=7ms TTL=57

Estadísticas de ping para 96.6.196.22:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 6ms, Máximo = 8ms, Media = 7ms

C:\Users\aliag>
```

Cuando hace ping a ***www.cisco.com***, ¿obtiene la misma dirección IP que la del ejemplo? Explique.
La respuesta varía según la ubicación geográfica. Cisco aloja su contenido web en una serie de servidores reflejados. Esto significa que Cisco carga exactamente el mismo contenido en varios servidores en diferentes partes del mundo. Cuando alguien intenta comunicarse con www.cisco.com, el tráfico se dirige al servidor espejo más cercano.
Escriba la dirección IP que obtuvo cuando hizo ping a www.cisco.com en un navegador. ¿Aparece el sitio web? Explique.
El sitio web de Cisco no se muestra. Hay, al menos, dos explicaciones posibles: 1. Algunos servidores web se configuran para que acepten direcciones IP que se envían desde un navegador; otros no. 2. Puede haber una regla de firewall en el sistema de seguridad de Cisco que prohíba el envío de una dirección IP a través de un navegador. Dependiendo del navegador web, también puede recibir un mensaje diciendo que la conexión no es segura o que hay un error de certificado.

Parte 2: Observe la búsqueda DNS mediante el comando nslookup en un sitio web

a. En el símbolo del sistema, escriba el comando **nslookup**. ¿Cuál es el servidor DNS predeterminado que se utiliza?

Rpta: Depende del sitio.

```
C:\Users\aliag>nslookup
Servidor predeterminado:  cachewas.tdp.net.pe
Address:  200.48.225.130

>
```

Observe que el símbolo del sistema cambió por el símbolo “mayor que” (>). Este es el símbolo de nslookup. Desde aquí, puede introducir comandos relacionados con el DNS. En el indicador, escriba ? para ver una lista de todos los comandos disponibles que puede usar en modo nslookup.

```
> ?
Comandos: (los identificadores se muestran en mayúsculas, [] significa opcional)
NOMBRE          - imprimir información acerca de NOMBRE de host o de dominio con el servidor predeterminado
NOMBRE1 NOMBRE2 - igual que el anterior, pero se usa NOMBRE2 como servidor
help o ?        - imprimir información acerca de comandos comunes
set OPCIÓN      - establecer una opción
    all                 - opciones de impresión, servidor actual y host
    [no]debug           - imprimir información de depuración
    [no]d2              - imprimir información de depuración exhaustiva
    [no]defname         - anexar el nombre de dominio a cada consulta
    [no]recurse         - pedir respuesta recursiva a la consulta
    [no]search          - usar la lista de búsqueda de dominios
    [no]vc              - usar siempre un circuito virtual
    domain=NOMBRE       - establecer nombre de dominio predeterminado en NOMBRE
    srchlist=N1[/N2/.../N6] - establecer dominio en N1 y lista de búsqueda en N1,N2, etc.
    root=NOMBRE         - establecer servidor raíz en NOMBRE
    retry=X             - establecer número de reintentos en X
    timeout=X           - establecer intervalo de tiempo de espera inicial en X segundos
    type=X              - establecer tipo de consulta (p. ej., A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
    querytype=X         - igual que type
    class=X             - establecer clase de consulta (p. ej., IN (Internet), ANY)
    [no]msxfr           - usar transferencia de zona rápida MS
    ixfrver=X           - versión actual que se usará en la solicitud de transferencia IXFR
server NOMBRE     - establecer el servidor predeterminado en NOMBRE con el servidor predeterminado actual
lserver NOMBRE    - establecer el servidor predeterminado en NOMBRE con el servidor inicial
root              - establecer el servidor predeterminado actual en la raíz
ls [opt] DOMINIO [> ARCHIVO] - enumerar las direcciones de DOMINIO (opcional: enviar el resultado a ARCHIVO)
    -a          -  enumerar nombres canónicos y alias
    -d          -  enumerar todos los registros
    -t TIPO     -  enumerar los registros del tipo de registro RFC dado (p. ej., A,CNAME,MX,NS,PTR etc.)
view ARCHIVO    - ordenar un archivo de resultados 'ls' y verlo con pg
exit            - salir del programa

> _
```

b. En el indicador de nslookup, escriba www.cisco.com.

```
> www.cisco.com
Servidor:  cachewas.tdp.net.pe
Address:  200.48.225.130

Respuesta no autoritativa:
Nombre:  e2867.dsca.akamaiedge.net
Addresses:  2600:1419:3200:181::b33
          2600:1419:3200:189::b33
          96.6.196.22
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net

>
```

¿Cuál es la dirección IPv4 traducida? Rpta: Desde una ubicación específica: 96.6.196.22

Nota: Lo más probable es que la dirección IP de su ubicación sea diferente porque Cisco usa servidores duplicados en varias ubicaciones en todo el mundo.

¿Es la misma dirección IP que aparece con el comando **ping**? Rpta: Sí.

En las direcciones, además de la dirección IP 96.6.196.22, hay los siguientes números: 2600:1419:3200:181::b33 y 2600:1419:3200:189:: b33. ¿De qué se trata? Rpta: Son las direcciones IP IPv6 (IP versión 6), en las que se puede acceder al sitio web.

c. En el indicador nslookup, escriba la dirección IP del servidor web de Cisco que acaba de encontrar. Si no conoce el URL, puede usar el comando nslookup para obtener el nombre de dominio de una dirección IP.

```
> 96.6.196.22
Servidor:  cachewas.tdp.net.pe
Address:  200.48.225.130

Nombre:  a96-6-196-22.deploy.static.akamaitechnologies.com
Address:  96.6.196.22

>
```

Puede utilizar la herramienta nslookup para traducir nombres de dominio a direcciones IP. También puede utilizarla para traducir direcciones IP a nombres de dominio.

Mediante la herramienta nslookup, registre las direcciones IP asociadas con www.google.com.

```
> www.google.com
Servidor:  cachewas.tdp.net.pe
Address:  200.48.225.130

Respuesta no autoritativa:
Nombre:  www.google.com
Addresses:  2800:3f0:4003:c08::67
          2800:3f0:4003:c08::69
          2800:3f0:4003:c08::93
          2800:3f0:4003:c08::63
          142.251.0.104
          142.251.0.103
          142.251.0.106
          142.251.0.147
          142.251.0.105
          142.251.0.99
```

Parte 3: Observar la búsqueda de DNS con el comando nslookup en **n** servidores de correo

a. En el indicador nslookup, escriba **set type=mx** para usar **nslookup** para identificar servidores de correo.

> **set type=mx**

b. En el indicador nslookup, escriba **cisco.com**.

```
> cisco.com
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
cisco.com MX preference = 20, mail exchanger = rcdn-mx-01.cisco.com
cisco.com MX preference = 30, mail exchanger = aer-mx-01.cisco.com
cisco.com MX preference = 10, mail exchanger = alln-mx-01.cisco.com
```

Un principio fundamental del diseño de red es la redundancia (la configuración de más de un servidor de correo). De esta manera, si no es posible acceder a uno de los servidores de correo, el equipo que realiza la consulta intenta con el segundo servidor. Los administradores de correo electrónico determinan qué servidor de correo se contacta primero utilizando la **preferencia MX**. Primero se contacta al servidor de correo con el valor de **MX preference** más bajo.

Pregunta: Según el resultado de la imagen de arriba, ¿qué servidor de correo se contactará primero cuando se envíe correo electrónico a cisco.com? Rpta: **alln-mx-01.cisco.com**

c. En el símbolo del sistema de nslookup, escriba **exit** para volver al símbolo del sistema normal del equipo.

d. En el símbolo del sistema, escriba **ipconfig /all**.

Escriba las direcciones IP de todos los servidores DNS que utilice su escuela.

Pregunta de reflexión: ¿Cuál es el propósito fundamental del DNS?

Rpta: DNS básicamente actúa como la guía telefónica para Internet. Por lo tanto, DNS traduce nombres a números. Los números pueden ser IPv4 o IPv6.

2. Servicios de DHCP

8.2.1 Protocolo de Configuración Dinámica de Host

El protocolo DHCP del servicio IPv4 automatiza la asignación de direcciones IPv4, máscaras de subred, gateways y otros parámetros de redes IPv4. Esto se denomina “direccionamiento dinámico”. La alternativa al direccionamiento dinámico es el direccionamiento estático. Al utilizar el direccionamiento estático, el administrador de redes introduce manualmente la información de la dirección IP en los hosts.

Cuando un host se conecta a la red, se realiza el contacto con el servidor de DHCP y se solicita una dirección. El servidor de DHCP elige una dirección de un rango de direcciones configurado llamado ***grupo*** y la asigna al host.

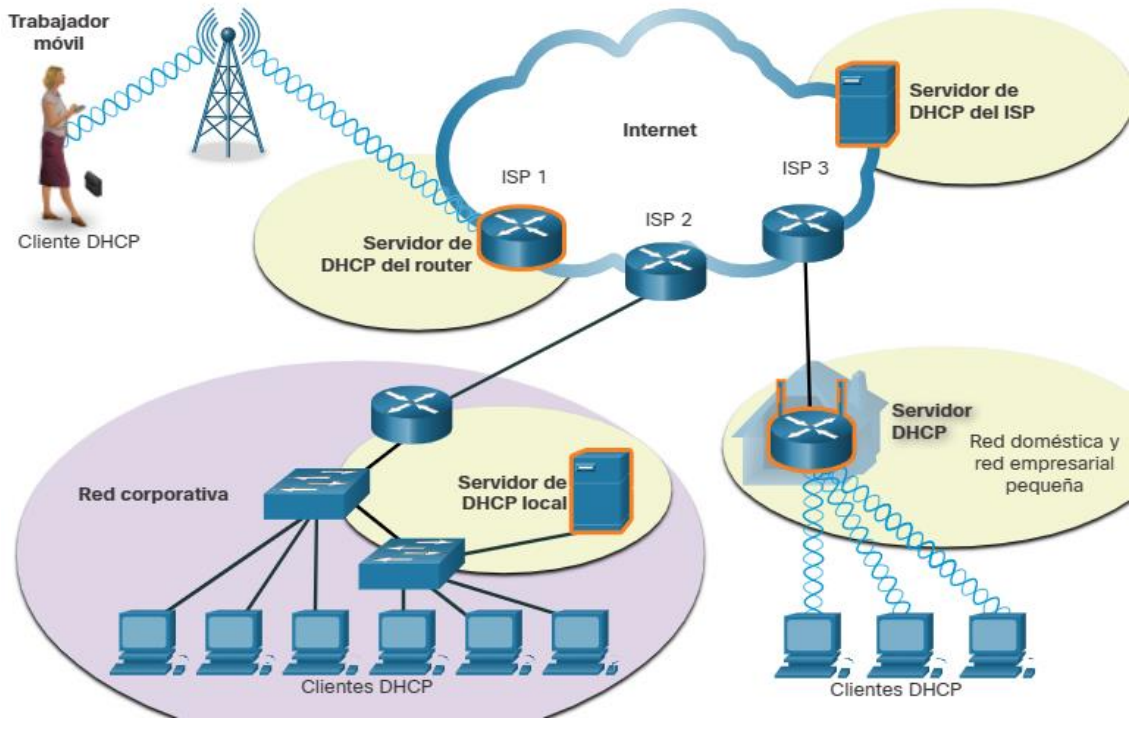
En redes más grandes, o donde los usuarios cambian con frecuencia, se prefiere asignar direcciones con DHCP. Es posible que los nuevos usuarios necesiten conexiones; otros pueden tener PC nuevas que deben estar conectadas. En lugar de usar asignación de direcciones estáticas para cada conexión, es más eficaz que las direcciones IPv4 se asignen automáticamente mediante DHCP.

DHCP puede asignar direcciones IP durante un período de tiempo configurable, denominado ***período de concesión***. El período de concesión es una configuración DHCP importante. Cuando caduca el período de concesión o el servidor DHCP recibe un mensaje ***DHCPRELASE***, la dirección se devuelve al grupo DHCP para su reutilización. Los usuarios pueden moverse libremente desde una ubicación a otra y volver a establecer con facilidad las conexiones de red por medio de DHCP.

Como lo muestra la figura, varios tipos de dispositivos pueden ser servidores DHCP. En la mayoría de las redes medianas a grandes, el servidor DHCP suele ser un servidor local y dedicado con base en una PC. En las redes domésticas, el servidor de DHCP suele estar ubicado en el router local que conecta la red doméstica al proveedor de servicio de internet (ISP).

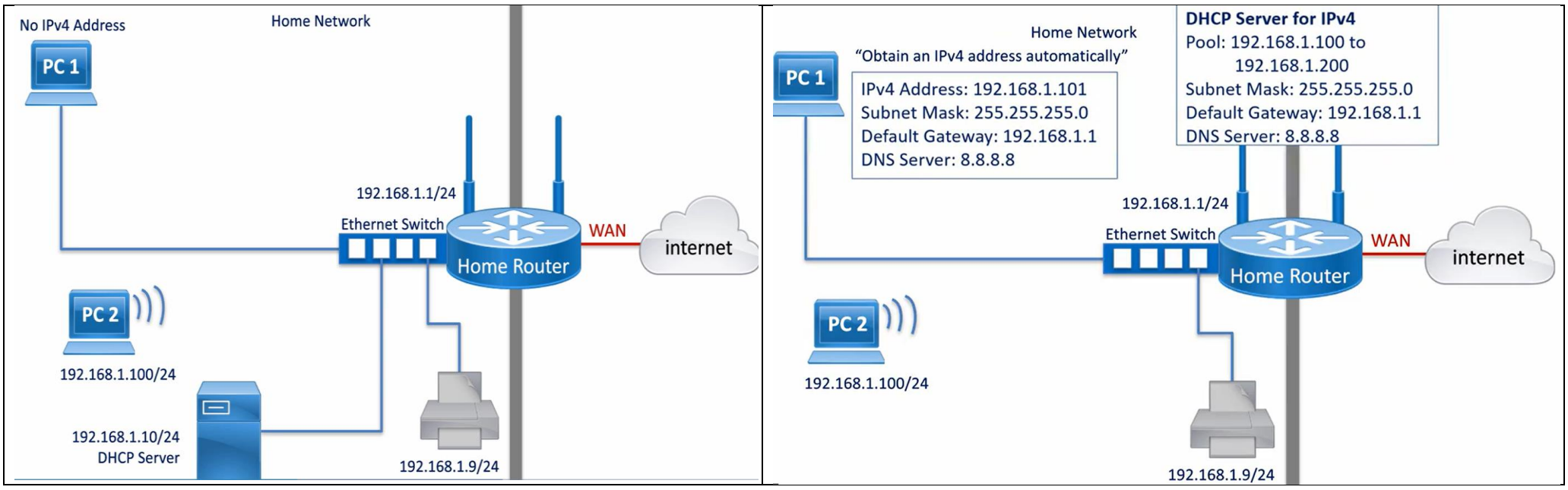
Muchas redes utilizan tanto el direccionamiento estático como DHCP. DHCP se utiliza para hosts de propósito general, tales como los dispositivos de usuario final. El direccionamiento estático se utiliza para los dispositivos de red, tales como enrutadores, puertas de enlace, conmutadores, servidores e impresoras.

DHCPv6 (DHCP para IPv6) proporciona servicios similares para los clientes IPv6. Una diferencia importante es que DHCPv6 no brinda una dirección de puerta de enlace predeterminada. Esto sólo se puede obtener de forma dinámica a partir del ***Router Advertisement*** (Anuncio de Enrutador) del propio enrutador.



8.2.2 Vídeo - Funcionamiento de DHCP en un Enrutador Doméstico

DHCP, o protocolo de configuración de host dinámico, es el servicio que permite que los dispositivos reciban automáticamente su dirección IP y otra información de direccionamiento desde un servidor DHCP. DHCP está disponible tanto para IPv4 como para IPv6. Existen algunas diferencias entre los dos, sin embargo, el resultado final es muy similar. En este video, nos enfocaremos en DHCP para IPv4, utilizando un enrutador doméstico típico como servidor DHCP. En nuestra topología puede ver que nuestro enrutador doméstico tiene la dirección IPv4 192.168.1.1 y también se ha habilitado como servidor DHCP. En lugar de un solo puerto para conectar nuestros dispositivos locales, la mayoría de los enrutadores domésticos incluyen un conmutador Ethernet incorporado. Dispositivos cliente como PC1 y PC2 normalmente recibirá su información de direccionamiento I Pv4 de un servidor DHCP. La PC2 ya recibió su información de direccionamiento mediante DHCP. Al asignar automáticamente la información de direccionamiento, DHCP elimina posibles problemas debido a errores de configuración manual. Sin embargo, es probable que algunos dispositivos, como una impresora o un servidor, tengan su información de direccionamiento IPv4 configurada manualmente. Esto es para garantizar que estos dispositivos tengan una dirección IPv4 específica. Un servidor DHCP puede ser una computadora separada, pero en el caso de la mayoría de las redes domésticas, el enrutador doméstico local actuará como un servidor DHCP. Entonces, en nuestro escenario, usaremos el enrutador doméstico como nuestro servidor DHCP. El enrutador doméstico se configuró como un servidor DHCP para proporcionar información de direccionamiento para los clientes, incluido el conjunto o alcance de las direcciones IPv4, normalmente direcciones IPv4 privadas. Cada cliente DHCP recibirá una dirección IPv4 única de este conjunto. El servidor DHCP realiza un seguimiento de qué dispositivo recibe qué dirección IPv4 asociando la dirección IPv4 asignada a la dirección Ethernet MAC del cliente. La máscara de subred, la puerta de enlace predeterminada y las direcciones del servidor DNS también se distribuyen y serán la misma información para todos los clientes. Como la mayoría de los dispositivos cliente, la PC1 está habilitada de forma predeterminada para obtener su IPv4 automáticamente mediante DHCP. El cliente enviará una transmisión Ethernet solicitando la dirección IPv4 desde un servidor DHCP. Después de una breve secuencia de mensajes entre el cliente y el servidor DHCP, el servidor asignará al cliente una de las direcciones IPv4 disponibles de su conjunto con la máscara de subred adecuada, la dirección de la puerta de enlace predeterminada y la dirección del servidor DNS. La PC1 ahora tiene su información de direccionamiento IPv4. Dado que uno de los clientes, la PC2, ya tiene la primera dirección del grupo, el servidor DHCP asigne la siguiente dirección disponible 192.168.1.101. Observe que la dirección de puerta de enlace predeterminada es la dirección del enrutador doméstico. El cliente ahora tiene toda la información de direccionamiento que necesita para comunicarse correctamente con los dispositivos en su propia red, así como con otros dispositivos, incluido Internet. Por cierto, así es como un enrutador doméstico recibe su información de direccionamiento IPv4 para su interfaz WAN, la interfaz que utiliza para conectarse al ISP. Cuando el Home Router está encendido, actúa como un cliente DHCP y recibe su dirección pública IPv4 y otra información de direccionamiento, del servidor DHCP de los ISPs, tal como vimos con la PC de nuestros clientes PC1.



8.2.3 Mensajes DHCP

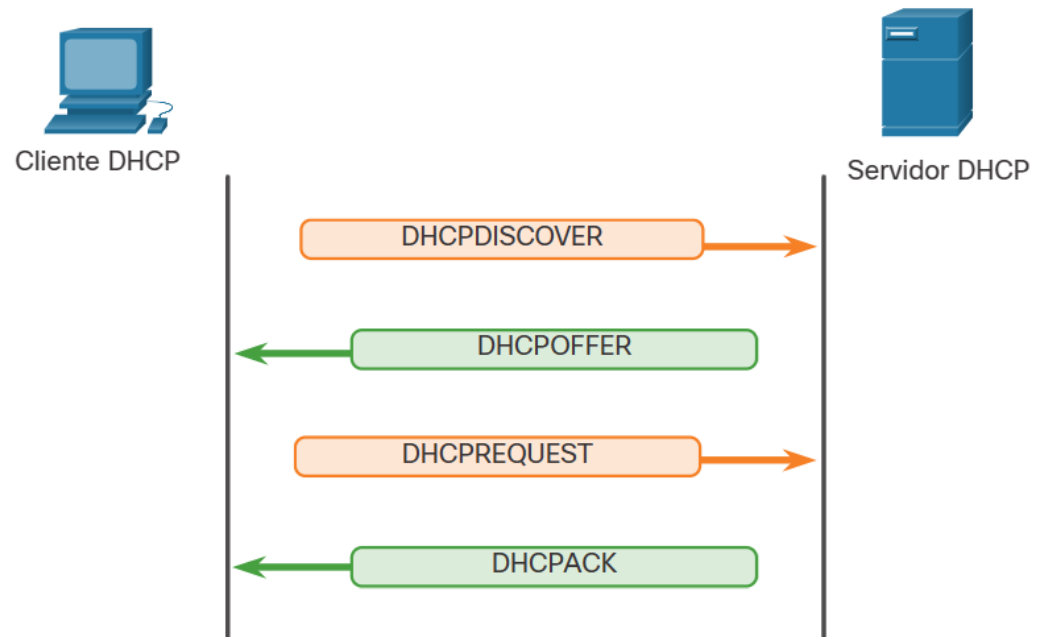
Como se muestra en la ilustración, cuando un dispositivo configurado con DHCP e IPv4 se inicia o se conecta a la red, el cliente transmite un mensaje de detección ***DHCPDISCOVER*** para identificar cualquier servidor de DHCP disponible en la red. Un servidor de DHCP responde con un mensaje de oferta ***DHCPOFFER***, que ofrece una concesión al cliente. El mensaje de oferta contiene la dirección IPv4 y la máscara de subred que se deben asignar, la dirección IPv4 del servidor DNS y la dirección IPv4 del gateway predeterminado. La oferta de concesión también incluye la duración de esta.

El cliente puede recibir varios mensajes DHCPOFFER si hay más de un servidor de DHCP en la red local. Por lo tanto, debe elegir entre ellos y enviar un mensaje de solicitud ***DHCPREQUEST*** que identifique el servidor explícito y la oferta de concesión que el cliente acepta. Un cliente también puede optar por solicitar una dirección previamente asignada por el servidor.

Suponiendo que la dirección IPv4 solicitada por el cliente, u ofrecida por el servidor, aún está disponible, el servidor devuelve un mensaje de reconocimiento ***DHCPACK*** que le informa al cliente que entregó la concesión. Si la oferta ya no es válida, el servidor seleccionado responde con un mensaje de reconocimiento negativo ***DHCPNAK***. Si se devuelve un mensaje DHCPNAK, entonces el proceso de selección debe volver a comenzar con la transmisión de un nuevo mensaje DHCPDISCOVER. Una vez que el cliente tiene la concesión, se debe renovar mediante otro mensaje DHCPREQUEST antes de que expire.

El servidor DHCP asegura que todas las direcciones IP sean únicas (no se puede asignar la misma dirección IP a dos dispositivos de red diferentes de forma simultánea). La mayoría de los proveedores de Internet utilizan DHCP para asignar direcciones a los clientes.

DHCPv6 tiene un conjunto similar de mensajes a los de DHCP para IPv4. Los mensajes DHCPv6 son ***SOLICIT, ADVERTISE, INFORMATION REQUEST y REPLY***.



8.2.4 Verifique su Comprensión - Servicios de DHCP

¿Verdadero o falso? Los clientes DHCP inician el proceso DHCP enviando un mensaje DHCPREQUEST a los servidores DHCP disponibles.

VERDADERO	FALSO ☺←

Hay cuatro mensajes DHCP intercambiados entre clientes y servidores. El cliente inicia el proceso DHCP con un mensaje de detección DHCPDISCOVER a los servidores DHCP disponibles.

¿Cuál de las siguientes opciones describe mejor DHCP?

- DHCP automatiza el proceso para detectar la dirección MAC del destino.
- DHCP automatiza el proceso para detectar la dirección IP de un nombre de dominio.
- DHCP automatiza la asignación de direcciones IP, máscaras de subred, puertas de enlace y otros parámetros de red IPv4. ☺←
- DHCP automatiza la traducción de direcciones IP públicas y privadas.

DHCP automatiza la asignación de direcciones IP, máscaras de subred, puertas de enlace y otros parámetros de red IPv4. ARP automatiza el proceso de detección de la dirección MAC del destino. DNS automatiza el proceso para detectar la dirección IP de un nombre de dominio. NAT automatiza la traducción de direcciones privadas a direcciones públicas.

¿Cuál es el orden correcto de los mensajes en funcionamiento DHCP?

- DHCPDISCOVER, DHCPOFFER, DHCPNAK, DHCPREQUEST
- DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPNAK ☺←
- DHCPOFFER, DHCPREQUEST, DHCPDISCOVER, DHCPNAK
- DHCPREQUEST, DHCPDISCOVER, DHCPOFFER, DHCPNAK

3. Resumen de Servicios de Direccionamiento IP

8.3.1 ¿Qué Aprendí en este Módulo?

Servicios de direccionamiento IP

En las redes de datos, los dispositivos se etiquetan con direcciones IP numéricas para enviar y recibir datos a través de las redes. Los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible. El protocolo DNS define un servicio automatizado que coincide con los nombres de recursos que tienen la dirección de red numérica solicitada. Las comunicaciones del protocolo DNS utilizan un único formato llamado “mensaje”. Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Estos registros contienen el nombre, la dirección y el tipo de registro. Este formato de mensaje que se ve en la figura se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, para los mensajes de error y para la transferencia de información de registro de recursos entre servidores.

DNS utiliza nombres de domino para formar la jerarquía. La estructura de nombres se divide en zonas. Cada servidor DNS mantiene un archivo de base de datos específico y sólo es responsable de administrar las asignaciones de nombre a IP para esa pequeña porción de toda la estructura DNS. Cuando un servidor DNS recibe una solicitud para una traducción de nombre que no se encuentra dentro de esa zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para su traducción. DNS es escalable, porque la resolución de los nombres de hosts se distribuye entre varios servidores.

Los sistemas operativos informáticos cuentan con una herramienta llamada ***nslookup*** que permite que el usuario consulte de forma manual los servidores de nombres para resolver un nombre de host dado. Esta utilidad también puede utilizarse para solucionar los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres. Cuando se ejecuta el comando nslookup, se muestra el servidor DNS predeterminado configurado para su host. El nombre de un host o dominio se puede ingresar en el indicador de nslookup.

En redes más grandes, se prefiere asignar direcciones con DHCP. En lugar de usar asignación de direcciones estáticas para cada conexión, es más eficaz que las direcciones IPv4 se asignen automáticamente mediante DHCP. DHCP puede asignar direcciones IP durante un período de

tiempo configurable, denominado período de concesión. Cuando caduca el período de concesión o el servidor DHCP recibe un mensaje ***DHCPRELASE***, la dirección se devuelve al rango de DHCP para su reutilización. Los usuarios pueden moverse libremente desde una ubicación a otra y volver a establecer con facilidad las conexiones de red por medio de DHCP.

DHCPv6 proporciona servicios similares para los clientes IPv6. Una diferencia importante es que DHCPv6 no brinda una dirección de puerta de enlace predeterminada. Esto sólo se puede obtener de forma dinámica a partir del ***Router Advertisement*** (Anuncio de Enrutador) del propio enrutador.

Cuando un dispositivo configurado con DHCP e IPv4 se inicia o se conecta a la red, el cliente transmite un mensaje de detección ***DHCPDISCOVER*** para identificar cualquier servidor de DHCP disponible en la red.

Un servidor de DHCP responde con un mensaje de oferta ***DHCPOFFER***, que ofrece una concesión al cliente. El cliente envía un mensaje ***DHCPREQUEST*** que identifica el servidor específico y le arrenda una oferta que el cliente está aceptando

Suponiendo que la dirección IPv4 solicitada por el cliente u ofrecida por el servidor aún está disponible, el servidor devuelve un mensaje ***DHCPACK*** que reconoce al cliente que el arrendamiento ha finalizado. Si la oferta ya no está disponible, entonces el servidor seleccionado responde con un mensaje ***DHCPNAK***. Si se devuelve un mensaje DHCPNAK, entonces el proceso de selección debe volver a comenzar con la transmisión de un nuevo mensaje DHCPDISCOVER.

DHCPv6 tiene un conjunto similar de mensajes a los de DHCP para IPv4. Los mensajes de DHCPv6 son ***SOLICIT, ADVERTISE, INFORMATION REQUEST y REPLY***.

8.3.2 Webster - Preguntas de Reflexión

¡Otro módulo más! ¿Qué aprendió en este módulo sobre los servicios de direccionamiento IP? Antes de tomar este módulo, ¿pensó en el protocolo DNS que define un servicio automatizado que hace coincidir los nombres de los recursos con la dirección de red numérica requerida? ¿Sabía la diferencia entre direccionamiento estático y DHCP? Realmente aprendí mucho y espero que ustedes también.

8.3.3 Prueba de Servicios de Direccionamiento IP

¿Qué servicio de red asigna automáticamente direcciones IP a los dispositivos en la red?

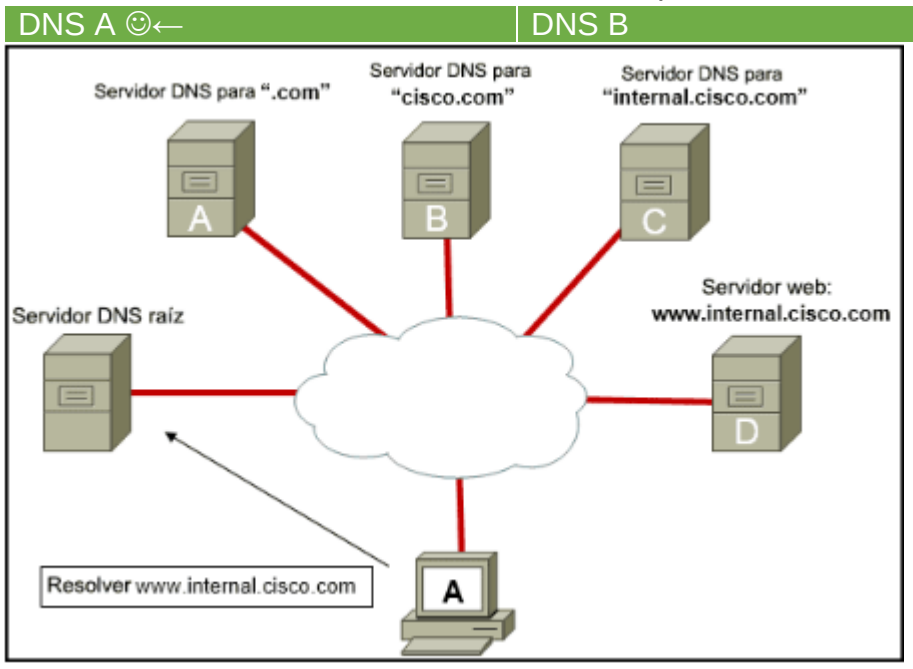
DHCP ☺←	TELNET	DNS	TRACEROUTE

Una PC acaba de iniciarse y está intentando obtener una dirección a través de DHCP. ¿Cuáles dos mensajes transmitirá generalmente el cliente en la red? (Escoja dos opciones).

DHCPDISCOVER ☺←	DHCPOFFER	DHCPREQUEST ☺←	DHCPACK	DHCPNACK

Consultar la ilustración. El host A está intentando resolver el nombre www.internal.cisco.com a una dirección IP. Cuando un servidor DNS raíz recibe la solicitud de resolución de nombre, ¿qué servidor se incluirá en la respuesta para una resolución adicional?

DNS A ☺←	DNS B	DNS C	DNS D



¿Qué afirmación es verdadera sobre el funcionamiento de DHCP?

Si el cliente recibe varios mensajes DHCPOFFER de diferentes servidores, envía un mensaje DHCPREQUEST de unidifusión al servidor desde el que elige obtener la información de IP.
Un cliente debe esperar el vencimiento de la concesión antes de enviar otro mensaje DHCPREQUEST.
Cuando un dispositivo que está configurado para usar DHCP arranca, el cliente transmite un mensaje DHCPDISCOVER para identificar cualquier servidor DHCP disponible en la red. ☺←
El mensaje DHCPDISCOVER contiene la dirección IP y la máscara de subred que se asignarán, la dirección IP del servidor DNS y la dirección IP del gateway predeterminado.

¿Qué mensaje DHCPv4 enviará un cliente para aceptar una dirección IPv4 ofrecida por un servidor DHCP?

DHCPACK de unidifusión	DHCPACK de difusión
DHCPREQUEST de unidifusión	DHCPREQUEST de difusión ☺←

Cuando un cliente DHCP recibe mensajes DHCPOFFER, enviará un mensaje de difusión DHCPREQUEST para dos propósitos. Primero, le indicará al servidor DHCP de oferta que desea aceptar la oferta y vincular la dirección IP. Segundo, le notifica a cualquier otro servidor DHCP de respuesta que sus ofertas se rechazan.

¿Qué protocolo traduce un nombre de sitio web como **www.cisco.com** en una dirección de red?

HTTP	FTP	DHCP	DNS ☺←

¿Qué tipo de información contiene un registro MX de DNS?

El FQDN del alias que se utiliza para identificar un servicio	La dirección IP para una entrada de FQDN
El nombre de dominio asignado a los servidores de intercambio de correos ☺←	La dirección IP de un servidor de nombres autoritativo

Un técnico está agregando una nueva PC a una LAN. Después de desempaquetar los componentes y realizar todas las conexiones, enciende la PC. Una vez que se carga el SO, el técnico abre un navegador y verifica que la PC tiene conexión a Internet. ¿Por qué pudo la PC conectarse a la red sin configuraciones adicionales?

- La PC no requiere ninguna información adicional para funcionar en la red.
- La PC vino preconfigurada de fábrica con información de asignación de direcciones IP.
- La PC está preconfigurada para utilizar DHCP. ☺←
- La PC utilizó DNS para recibir automáticamente información de asignación de direcciones IP de un servidor.
- La interfaz virtual de la PC es compatible con cualquier red.

¿Qué servidor de red no funciona correctamente si un usuario puede hacer ping a la dirección IP de un servidor web, pero no puede hacer ping al nombre de host del servidor web?

DNS ☺←	DHCP	FTP	HTTP

Consulte la ilustración. ¿Qué protocolo permite que un usuario escriba www.cisco.com en lugar de una dirección IP para acceder al servidor web?

DNS ☺←	FTP	HTML	HTTP	SNMP

¿Qué acción realiza un servidor DNS si no tiene una entrada para una URL solicitada?

El servidor descarta la solicitud.	El servidor devuelve una respuesta de "no se encontró la página" al cliente.
El servidor consulta a otro servidor DNS para ver si tiene una entrada. ☺←	El servidor asigna una dirección IP temporaria al nombre y le envía esta dirección IP al cliente.

Módulo 9: La Capa de Transporte

0. Introducción

9.0.1 Webster - ¿Por Qué Debería Tomar este Módulo?

Parece que Olcay y Abay están terminando su turno en la planta de servicios públicos. Olcay le dice a Abay que tenga buenas noches. Ella le dice que esté preparado para hablar sobre todas las cosas que tienen que ver con la capa de transporte por la mañana.

Abay podría tomar este módulo antes de hablar con Olcay por la mañana. ¿Está familiarizado con la capa de transporte? Debería serlo si desea comprender las redes. La capa de transporte es responsable de las comunicaciones lógicas entre aplicaciones que se ejecutan en diferentes hosts. ¡Comencemos con este módulo para aprender más!

9.0.2 ¿Qué Voy a Aprender en este Módulo?

- **Título del Módulo: La Capa de Transporte**
- **Objetivo del Módulo**: Comparar las operaciones de los protocolos de la capa de transporte en el soporte de la comunicación de extremo a extremo.

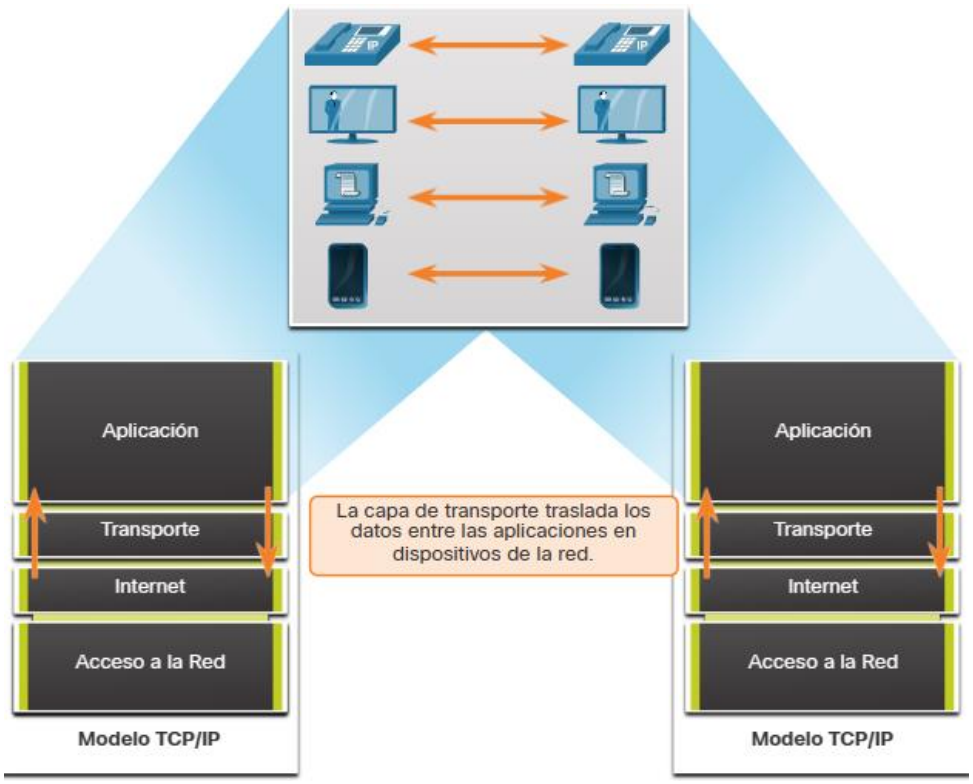
Título del Tema	Objetivo del Tema
Transporte de Datos	Explique el propósito de la capa de transporte en la administración del transporte de datos en la comunicación de extremo a extremo.
Descripción General de TCP	Explicar las características de TCP.
Descripción General de UDP	Explicar las características de UDP.
Números de Puerto	Explique cómo TCP y UDP usan los números de puerto.
Proceso de Comunicación TCP	Explique la forma en que los procesos de establecimiento y finalización de sesión TCP facilitan una comunicación confiable.
Confiabilidad y Control de Flujo	Explique la forma en que se transmiten y se reconocen las unidades de datos del protocolo TCP para garantizar la entrega.
Comunicación UDP	Describa los procesos de cliente UDP para establecer la comunicación con un servidor.

1. Transporte de datos

9.1.1 Función de la Capa de Transporte

Los programas de la capa Aplicación generan datos que deben intercambiarse entre los hosts de origen y de destino. La capa Transporte es responsable de las comunicaciones lógicas entre aplicaciones que se ejecutan en diferentes hosts. Esto puede incluir servicios como el establecimiento de una sesión temporal entre dos hosts y la transmisión fiable de información para una aplicación.

Como se muestra en la ilustración, la capa Transporte es el enlace entre la capa Aplicación y las capas inferiores que son responsables de la transmisión a través de la red.



La capa Transporte no tiene conocimiento del tipo de host destino, el tipo de medio por el que viajan los datos, la ruta tomada por los datos, la congestión en un enlace o el tamaño de la red. La capa Transporte incluye dos protocolos:

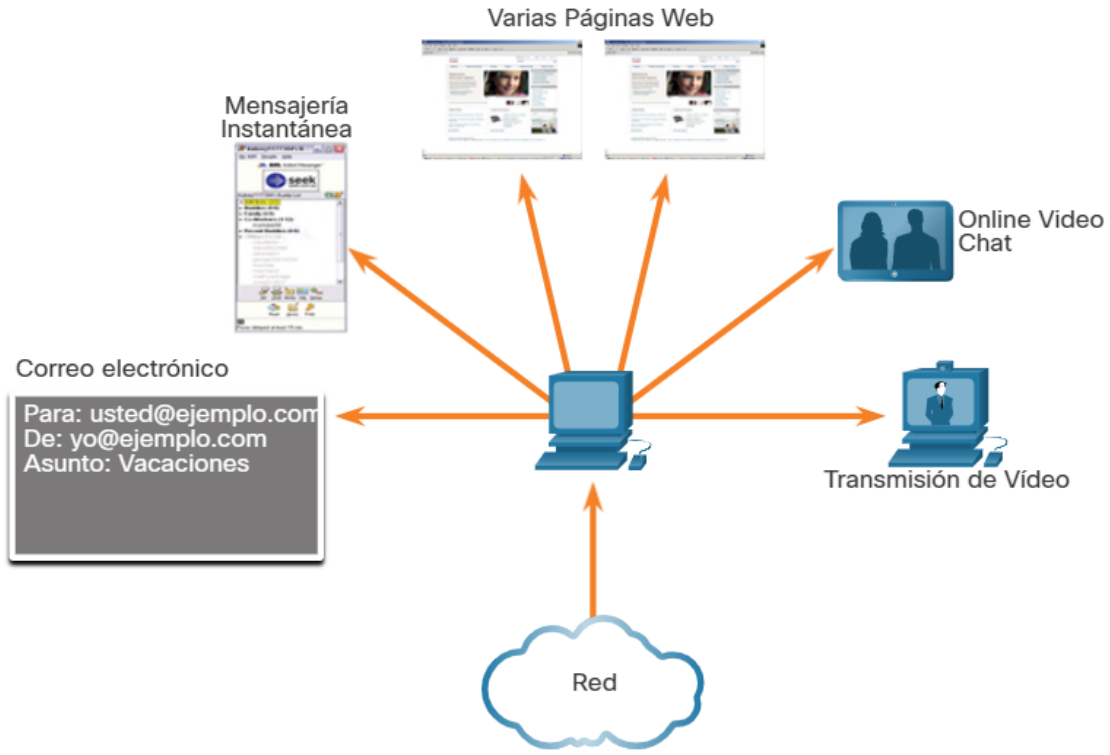
- Protocolo de control de transmisión (TCP)
- Protocolo de datagramas de usuario (UDP)

9.1.2 Tareas de la capa Transporte

Seguimiento de Conversaciones Individuales

En la capa Transporte, cada conjunto de datos que fluye entre una aplicación de origen y una aplicación de destino se conoce como una conversación y se rastrea por separado. Es responsabilidad de la capa Transporte mantener y hacer un seguimiento de todas estas conversaciones. Como se ilustra en la figura, un host puede tener múltiples aplicaciones que se comunican a través de la red simultáneamente.

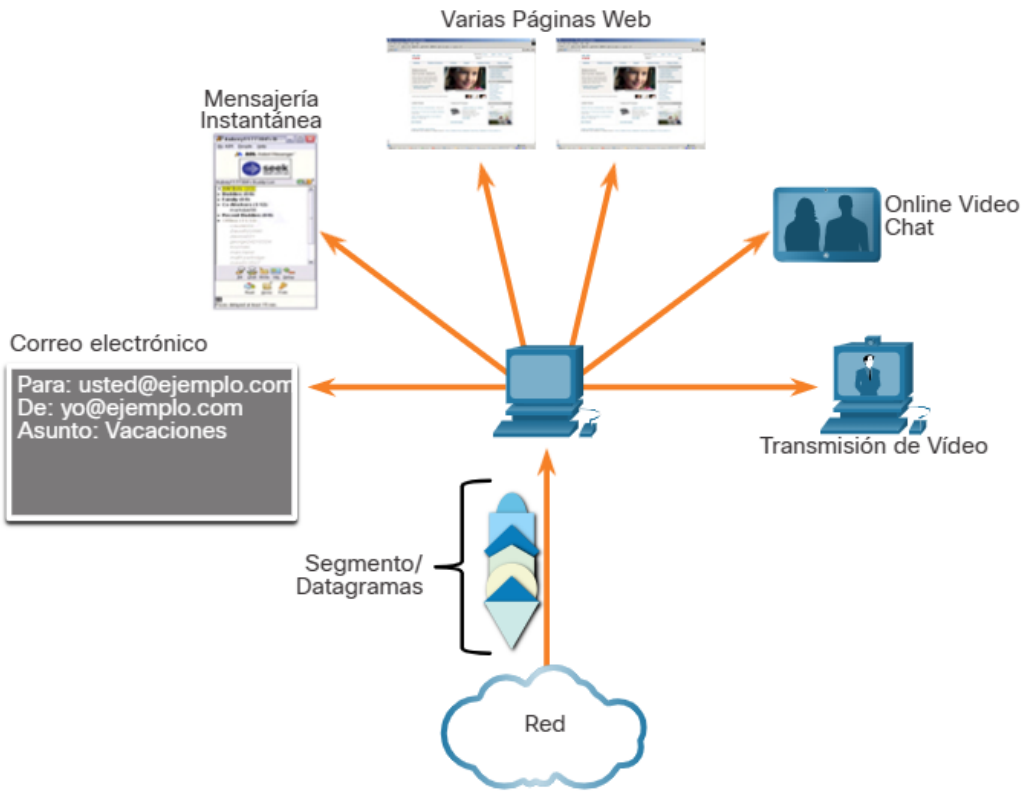
La mayoría de las redes tienen un límite en la cantidad de datos que se puede incluir en un solo paquete. Por lo tanto, los datos deben dividirse en piezas manejables.



Segmentación de Datos y Rearmado de Segmentos

Es responsabilidad de la capa Transporte dividir los datos de la aplicación en bloques de tamaño adecuado. Dependiendo del protocolo de capa Transporte utilizado, sus bloques se denominan segmentos o datagramas. La figura ilustra la capa Transporte utilizando diferentes bloques para cada conversación.

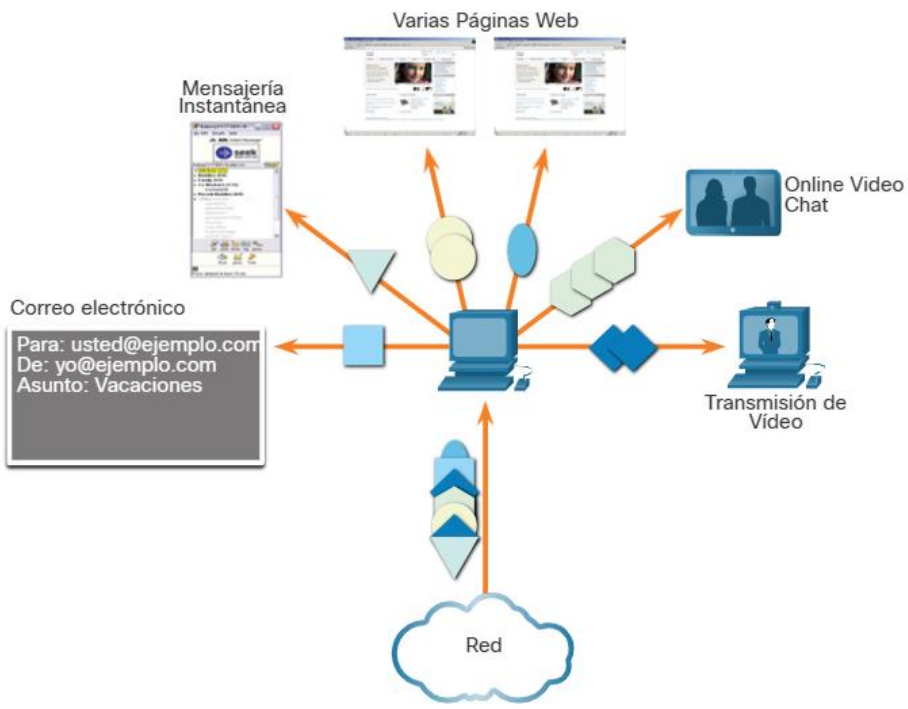
La capa Transporte divide los datos en bloques más pequeños (es decir, segmentos o datagramas) que son más fáciles de administrar y transportar.



Agregar Información de Encabezado

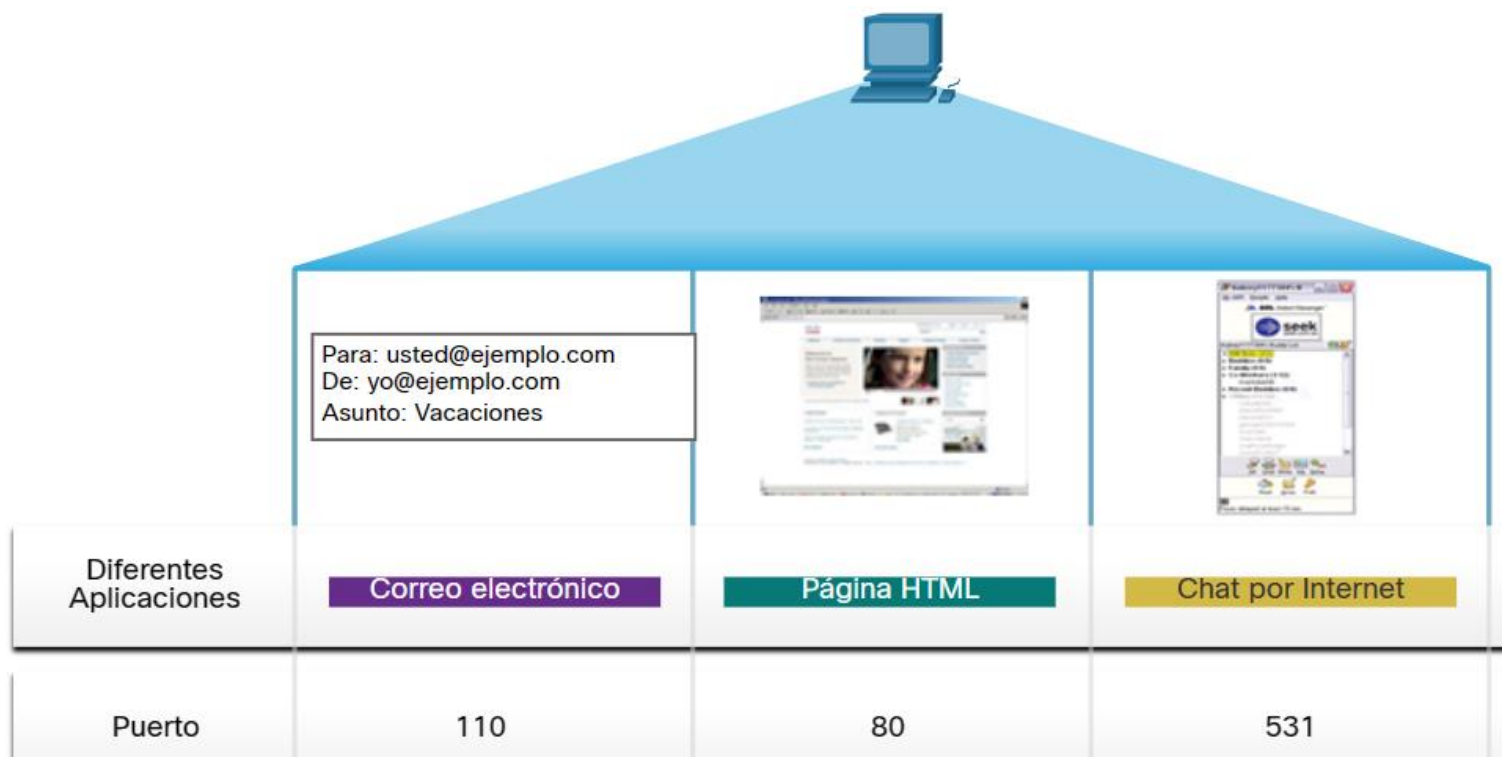
El protocolo de la capa Transporte también agrega información de encabezado -que contiene datos binarios organizados en varios campos- a cada bloque de datos. Los valores de estos campos permiten que los distintos protocolos de la capa Transporte lleven a cabo variadas funciones de administración de la comunicación de datos. Por ejemplo, el host receptor utiliza la información de encabezado para volver a ensamblar los bloques de datos en un flujo completo para el programa de la capa Aplicación de recepción.

La capa Transporte garantiza que incluso con múltiples aplicaciones que se ejecutan en un dispositivo, todas las aplicaciones reciban los datos correctos.



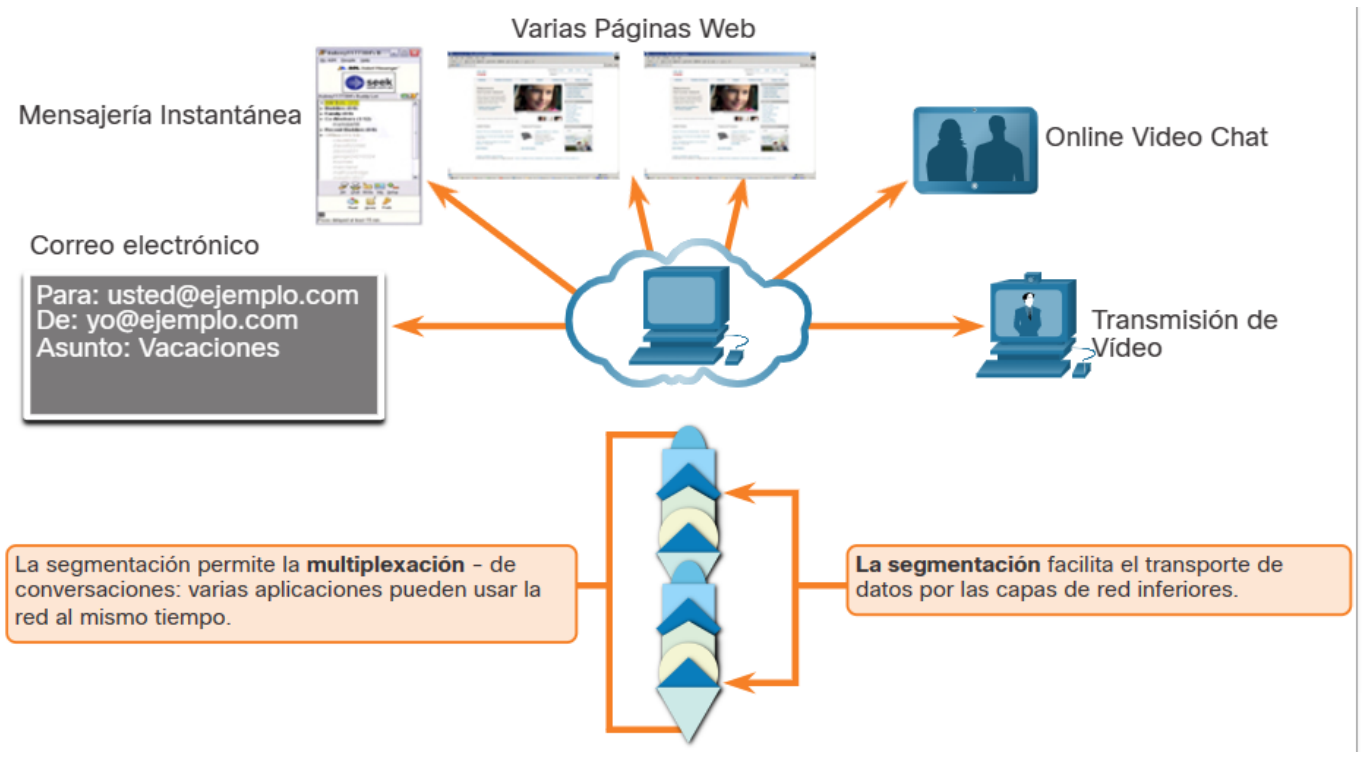
Identificación de las Aplicaciones

La capa Transporte separa y administra varias comunicaciones con diferentes requisitos. Para pasar flujos de datos a las aplicaciones adecuadas, la capa Transporte identifica la aplicación de destino utilizando un identificador llamado ***número de puerto***. Como se ilustra en la figura, a cada proceso de software que necesita acceder a la red se le asigna un número de puerto único para ese host.



Multiplexación de Conversaciones
El envío de algunos tipos de datos (por ejemplo, una transmisión de video) a través de una red, como una transmisión de comunicación completa, puede consumir todo el ancho de banda disponible. Esto impide que se produzcan otras conversaciones de comunicación al mismo tiempo. También podría dificultar la recuperación de errores y la retransmisión de datos dañados. Como se muestra en la figura, la capa Transporte utiliza segmentación y multiplexación para permitir que diferentes conversaciones de comunicación se intercalen en la misma red.

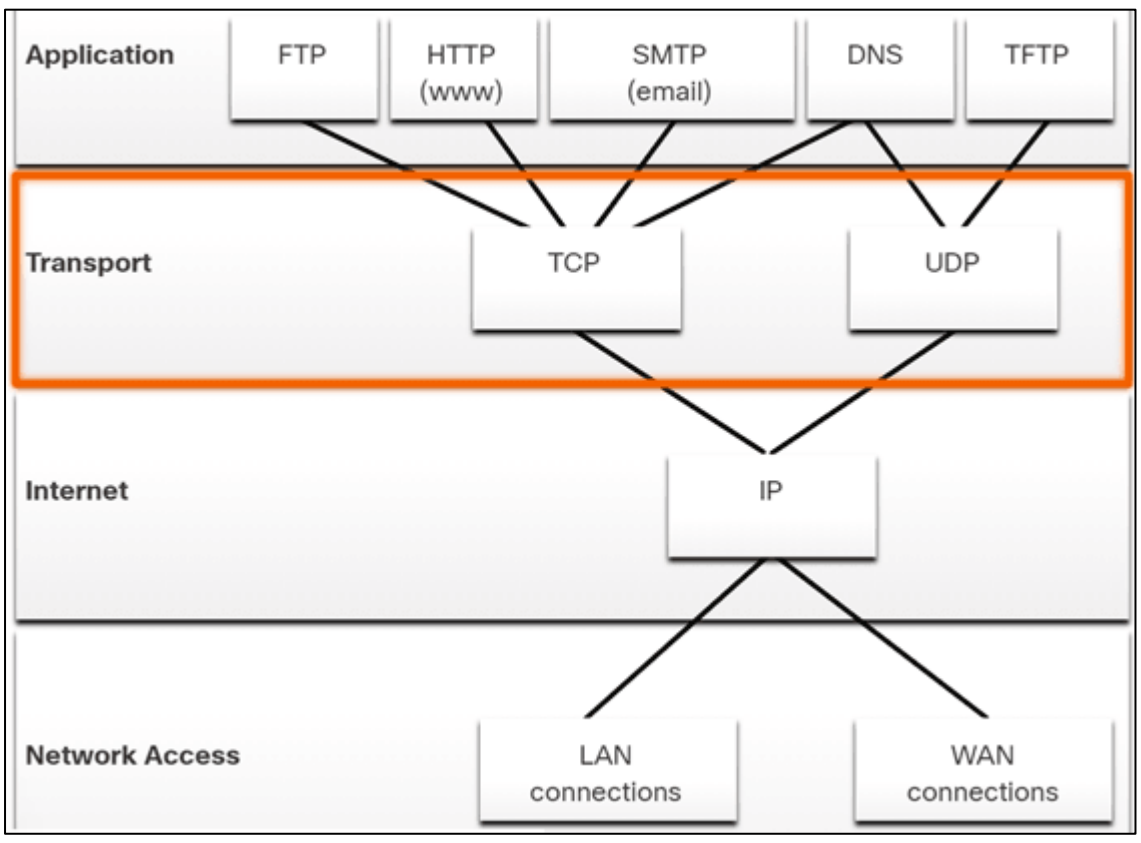
La verificación de errores se puede realizar en los datos del segmento, para determinar si el segmento se modificó durante la transmisión.



9.1.3 Protocolos de la capa Transporte

IP se ocupa solo de la estructura, direccionamiento y routing de paquetes. IP no especifica la manera en que se lleva a cabo la entrega o el transporte de los paquetes. Los protocolos de la capa Transporte especifican cómo transferir mensajes entre hosts y son responsables de administrar los requisitos de fiabilidad de una conversación. La capa Transporte incluye los protocolos ***TCP y UDP***.

Las diferentes aplicaciones tienen diferentes requisitos de confiabilidad de transporte. Por lo tanto, ***TCP/IP*** proporciona dos protocolos en la capa Transporte, TCP y UDP, como se muestra en la figura.



9.1.4 Protocolo de Control de Transmisión (TCP)

IP solo se refiere a la ***estructura, direccionamiento y enrutamiento de paquetes***, desde el remitente original hasta el destino final. IP no es responsable de garantizar la entrega o determinar si es necesario establecer una conexión entre el remitente y el receptor.

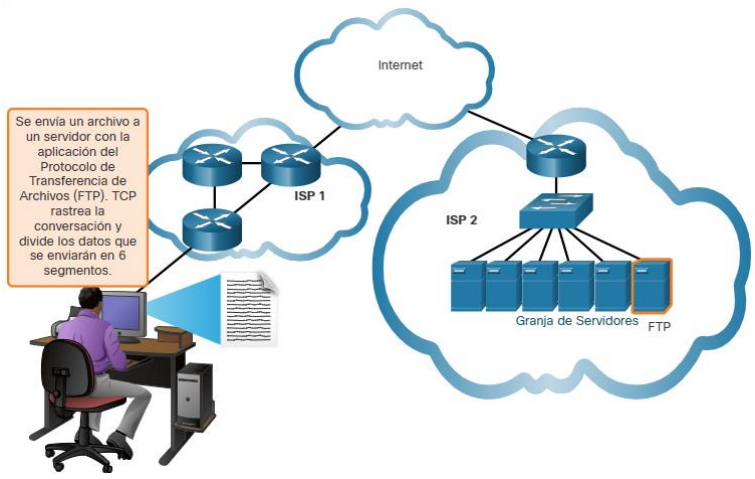
El TCP se considera un protocolo confiable y completo de la capa Transporte, garantiza que todos los datos lleguen al destino. TCP incluye campos que garantizan la entrega de los datos de la aplicación. Estos campos requieren un procesamiento adicional por parte de los hosts de envío y recepción. **Nota:** TCP divide los datos en ***segmentos***.

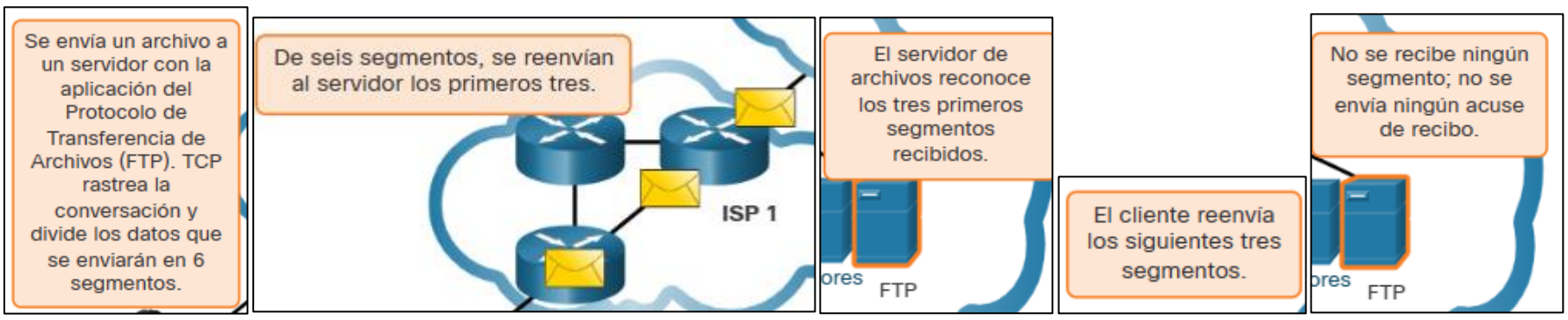
La función del protocolo TCP es similar al envío de paquetes a los que se hace un rastreo de origen a destino. Si se divide un pedido de envío en varios paquetes, un cliente puede verificar en línea para ver el orden de la entrega.

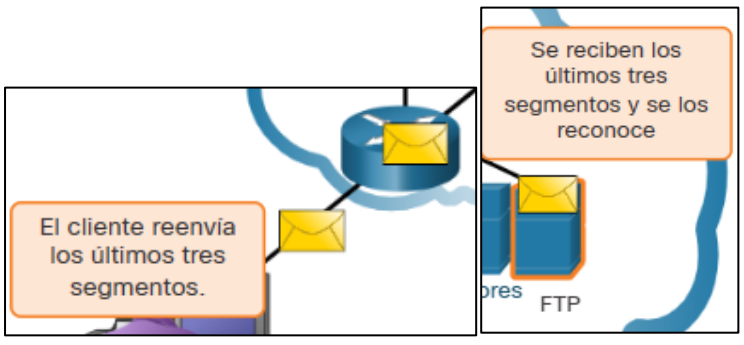
TCP proporciona confiabilidad y control de flujo mediante estas operaciones básicas:

- Numera y rastrea segmentos de datos transmitidos a un host específico desde una aplicación específica
- Confirma acuses de recibidos
- Vuelve a transmitir cualquier información no reconocida después de un cierto período de tiempo
- Retransmite datos de secuencia que pueden llegar en un orden incorrecto
- Envía datos a una velocidad eficiente que sea aceptable por el receptor

Para mantener el estado de una conversación y realizar un seguimiento de la información, TCP primero establece una conexión entre el remitente y el receptor. Es por eso que TCP se conoce como un ***protocolo orientado a la conexión***.







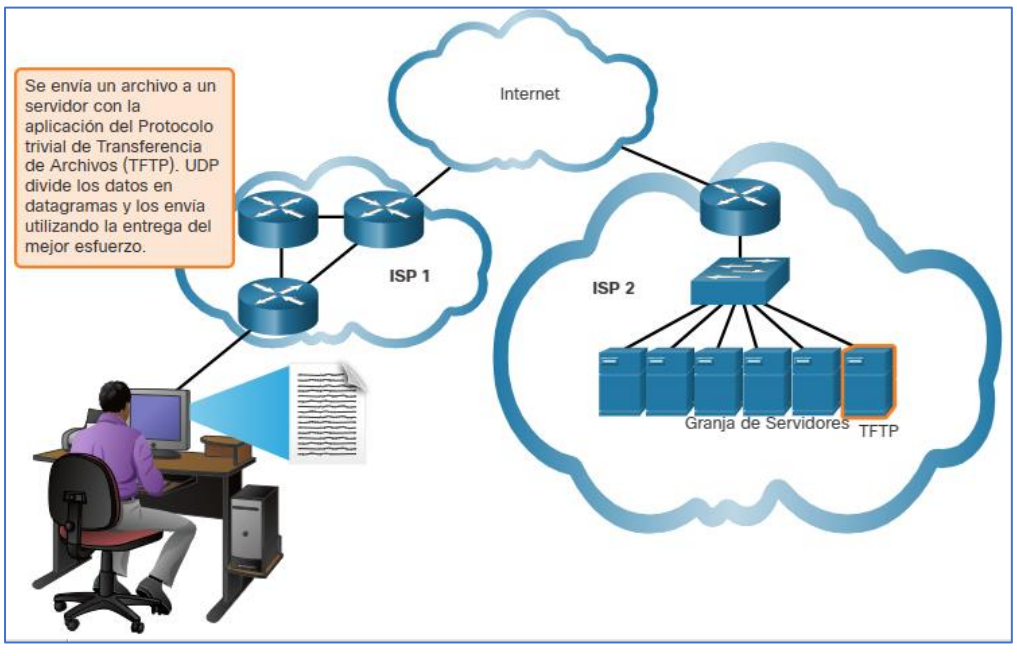
9.1.5 Protocolo Datagramas de Usuario (UDP)

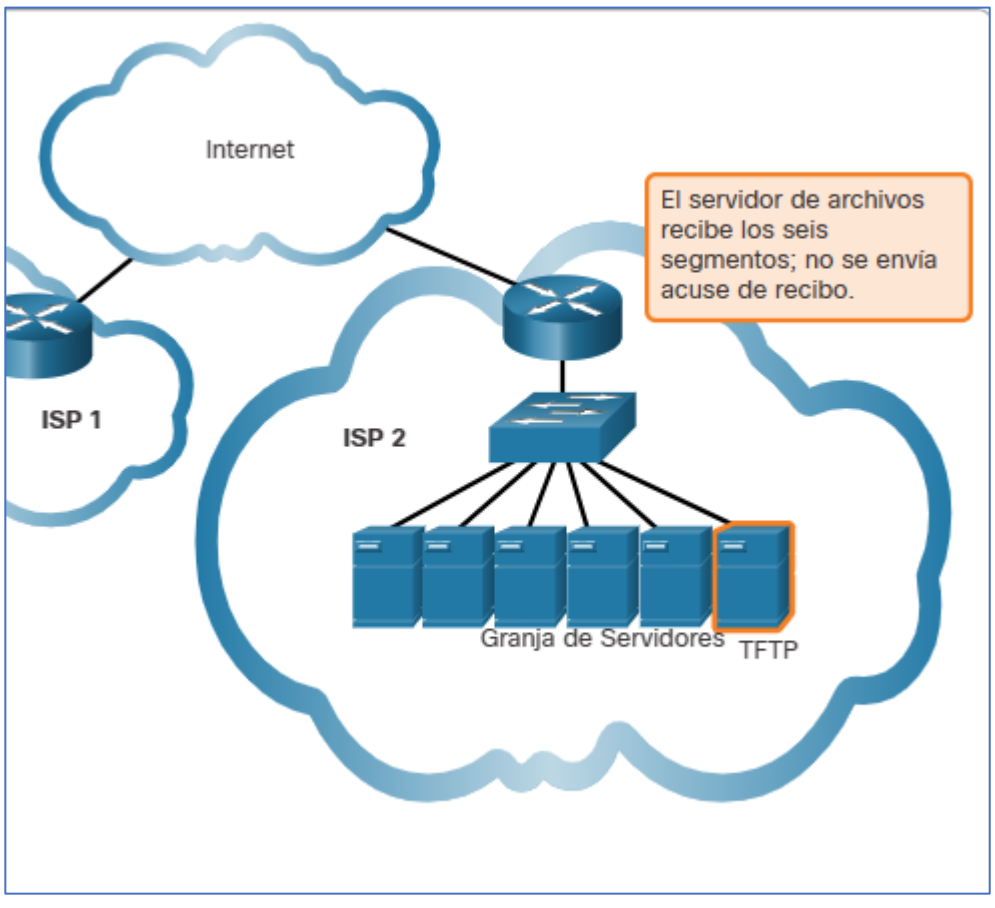
UDP es un protocolo de capa de transporte más simple que TCP. No proporciona confiabilidad y control de flujo, lo que significa que requiere menos campos de encabezado. Debido a que los procesos UDP remitente y receptor no tienen que administrar la confiabilidad y el control de flujo, significa que los datagramas UDP se pueden procesar más rápido que los segmentos TCP. El UDP proporciona las funciones básicas para entregar segmentos de datos entre las aplicaciones adecuadas, con muy poca sobrecarga y revisión de datos. **Nota:** UDP divide los datos en ***datagramas*** que también se conocen como segmentos.

UDP es un protocolo sin conexión, no requiere una conexión establecida, no proporciona fiabilidad ni control de flujo. Debido a que UDP no realiza un seguimiento de la información enviada o recibida entre el cliente y el servidor, UDP también se conoce como ***protocolo sin estado***.

UDP también se conoce como un ***protocolo de mejor esfuerzo en la entrega*** porque no sabe si los datos se entregan al destino. Con UDP, no existen procesos en la capa Transporte que informen al emisor si la entrega se realizó correctamente.

UDP es como colocar una carta común, no registrada, en el correo. El emisor de la carta no conoce la disponibilidad del receptor para recibir la carta. Además, la oficina de correos tampoco es responsable de hacer un rastreo de la carta ni de informar al emisor si esta no llega a destino.





9.1.6 El Protocolo de capa Transporte adecuado para la aplicación adecuada

Algunas aplicaciones como Voz sobre IP (VoIP) pueden tolerar pérdida de datos durante la transmisión a través de la red, pero los retrasos son inaceptables. Para estas aplicaciones, UDP es la mejor opción porque requiere menos sobrecarga de red. Los reconocimientos y la retransmisión retrasarían la entrega y harían inaceptable la conversación de voz.

UDP también es utilizado por las aplicaciones de solicitud y respuesta donde los datos son mínimos, y la retransmisión se puede hacer rápidamente. Por ejemplo, el Sistema de Nombres de Dominio (DNS) utiliza UDP para este tipo de transacción. El cliente solicita direcciones IPv4 e IPv6 para obtener un nombre de dominio conocido desde un servidor DNS. Si el cliente no recibe una respuesta en un período de tiempo predeterminado, simplemente envía la solicitud de nuevo.

Por ejemplo, si uno o dos segmentos de una transmisión de vídeo en vivo no llegan al destino, se interrumpe momentáneamente la transmisión. Esto puede manifestarse como distorsión en la imagen o el sonido, pero puede no ser perceptible para el usuario. Si el dispositivo de destino tuviera que dar cuenta de los datos perdidos, la transmisión se podría demorar mientras espera las retransmisiones, lo que ocasionaría que la imagen o el sonido se degraden considerablemente. En este caso, es mejor producir el mejor vídeo o audio posible con los segmentos recibidos y prescindir de la confiabilidad.

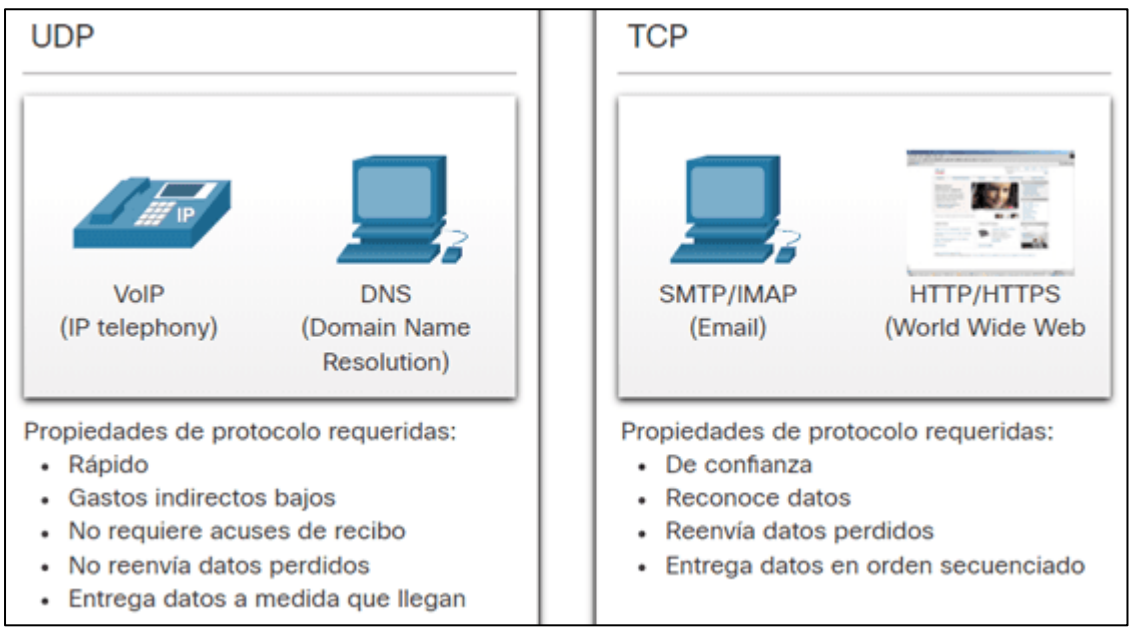
Para otras aplicaciones es importante que todos los datos lleguen y que puedan ser procesados en su secuencia adecuada. Para estos tipos de aplicaciones, TCP se utiliza como protocolo de transporte. Por ejemplo, las aplicaciones como las bases de datos, los navegadores web y los clientes de correo electrónico, requieren que todos los datos que se envían lleguen a destino en su formato original. Cualquier dato faltante podría corromper una comunicación, haciéndola incompleta o ilegible. Por ejemplo, cuando se accede a la información bancaria a través de la web, es importante asegurarse de que toda la información se envía y recibe correctamente.

Los desarrolladores de aplicaciones deben elegir qué tipo de protocolo de transporte es adecuado según los requisitos de las aplicaciones. El vídeo puede enviarse a través de TCP o UDP. Las aplicaciones que transmiten ***audio y video almacenado*** generalmente usan TCP. La aplicación utiliza TCP para realizar buffering, sondeo de ancho de banda y control de congestión, con el fin de controlar mejor la experiencia del usuario.

El ***audio y video en tiempo real*** generalmente usan UDP, pero también pueden usar TCP, o tanto UDP como TCP. Una aplicación de videoconferencia puede usar UDP de forma predeterminada, pero debido a que muchos firewalls bloquean UDP, la aplicación también se puede enviar a través de TCP.

Las aplicaciones que transmiten audio y video almacenado usan TCP. Por ejemplo, si de repente la red no puede admitir el ancho de banda necesario para ver una película a pedido, la aplicación detiene la reproducción. Durante la pausa, es posible que vea un mensaje de “almacenando en búfer...” mientras TCP intenta restablecer la transmisión. Cuando todos los segmentos están en orden y se restaura un nivel mínimo de ancho de banda, se reanuda la sesión TCP y se reanuda la reproducción de la película.

La figura resume las diferencias entre UDP y TCP.



9.1.7 Verifique su Comprensión - Transporte de Datos

¿Qué capa es responsable de establecer una sesión de comunicación temporal entre las aplicaciones host de origen y destino?

capa de aplicación
capa de enlace de datos
capa de red
capa física
capa de transporte ☺←

¿Cuáles son las tres responsabilidades de la capa de transporte? (Escoja tres opciones).

Multiplexión de conversaciones ☺←
identificación de marcos
identificación de información de enrutamiento
segmentación de datos y reensamblado de segmentos ☺←
Seguimiento de conversaciones individuales ☺←

¿Qué declaración de protocolo de capa de transporte es verdadera?

TCP tiene menos campos que UDP.	TCP es más rápido que UDP.
UDP es un protocolo de entrega de mejor esfuerzo. ☺←	UDP proporciona fiabilidad.

¿Cuál protocolo de la capa de transporte se usaría para aplicaciones VoIP?

Protocolo de Información de Sesión (SIP)	Protocolo de control de transmisión (TCP)
Protocolo de datagramas de usuario (UDP) ☺←	Protocolo de Transferencia VoIP

2. Descripción general de TCP

9.2.1 Características de TCP

En el tema anterior, aprendió que TCP y UDP son los dos protocolos de la capa Transporte. Este tema proporciona más detalles sobre lo que hace TCP y cuándo es una buena idea usarlo en lugar de UDP. Para comprender las diferencias entre TCP y UDP, es importante comprender cómo cada protocolo implementa funciones de confiabilidad específicas y cómo cada protocolo rastrea las conversaciones.

Además de admitir las funciones básicas de segmentación y reensamblado de datos, TCP también proporciona los siguientes servicios:

- **Establece una sesión** - TCP es un protocolo orientado a la conexión que negocia y establece una conexión permanente (o sesión) entre los dispositivos de origen y destino antes de reenviar cualquier tráfico. Mediante el establecimiento de sesión, los dispositivos negocian la cantidad de tráfico que se puede reenviar en un momento determinado, y los datos que se comunican entre ambos se pueden administrar detenidamente.
- **Garantiza una Entrega Confiable** - Por muchas razones, es posible que un segmento se corrompa o se pierda por completo, ya que se transmite a través de la red. TCP asegura que cada segmento que envía la fuente llega al destino.
- **Proporciona Entrega en el Orden Correcto** - Debido a que las redes pueden proporcionar múltiples rutas que pueden tener diferentes velocidades de transmisión, los datos pueden llegar en el orden incorrecto. Al numerar y secuenciar los segmentos, TCP garantiza que los segmentos se vuelvan a ensamblar en el orden correcto.
- **Admite Control de Flujo** - Los hosts de red tienen recursos limitados (es decir, memoria y potencia de procesamiento). Cuando TCP advierte que estos recursos están sobrecargados, puede solicitar que la aplicación emisora reduzca la velocidad del flujo de datos. Esto lo lleva a un cabo TCP, que regula la cantidad de datos que transmite el origen. El control de flujo puede evitar la necesidad de retransmitir los datos cuando los recursos del host receptor se ven desbordados.

Para obtener más información sobre TCP, busque en Internet el RFC 793.

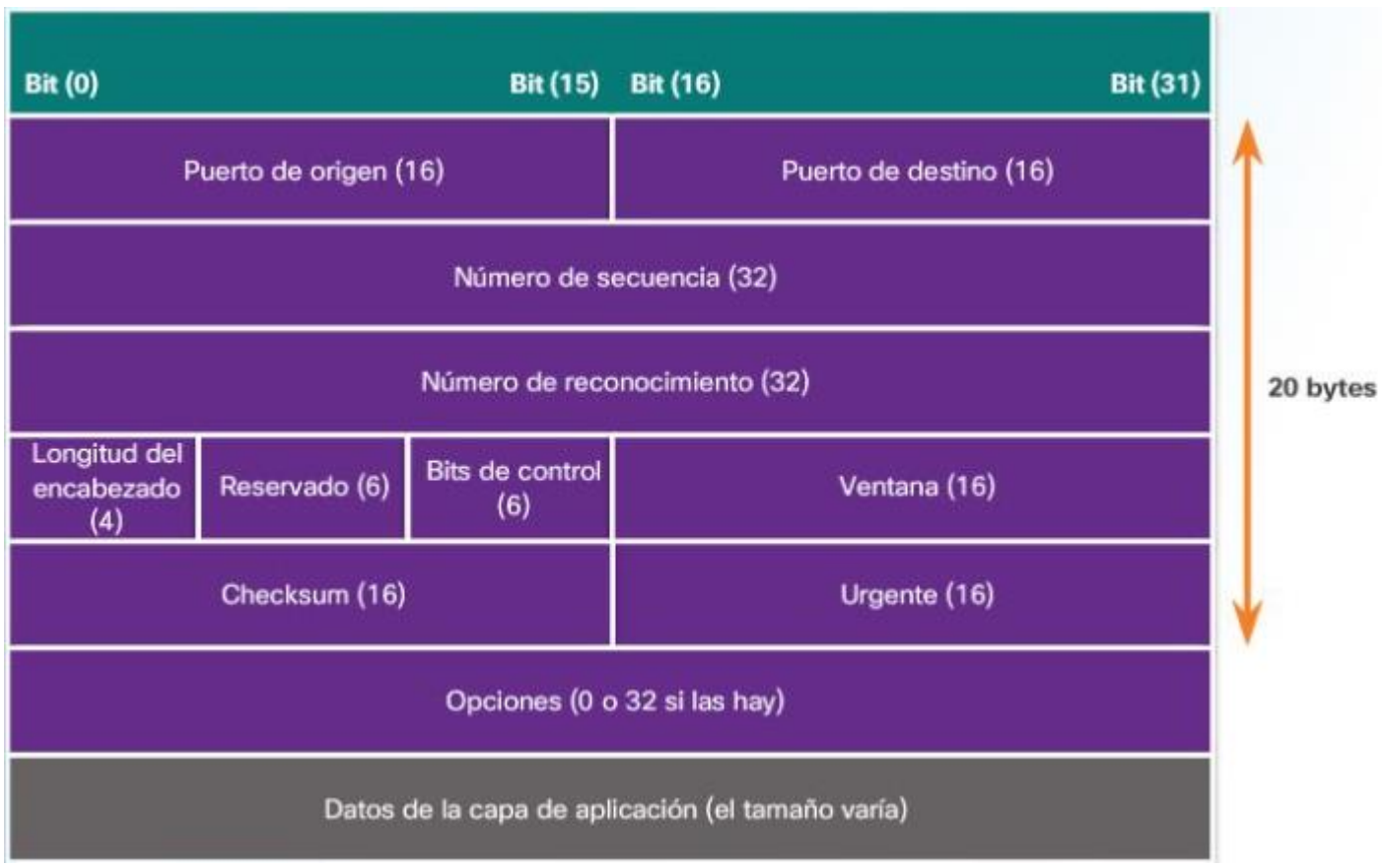
9.2.2 El Encabezado TCP

TCP es un ***protocolo con estado***, significa que realiza un seguimiento del estado de la sesión de comunicación. Para hacer un seguimiento del estado de una sesión, TCP registra qué información se envió y qué información se reconoció. La sesión con estado comienza con el establecimiento de la sesión y termina con la finalización de la sesión.

Un segmento TCP agrega 20 bytes (160 bits) de sobrecarga al encapsular los datos de la capa Aplicación.

La figura muestra los campos en un encabezado TCP.

(16+16+32+32+4+6+6+16+16+16=160 bits=8bytes)



9.2.3 Campos del Encabezado TCP

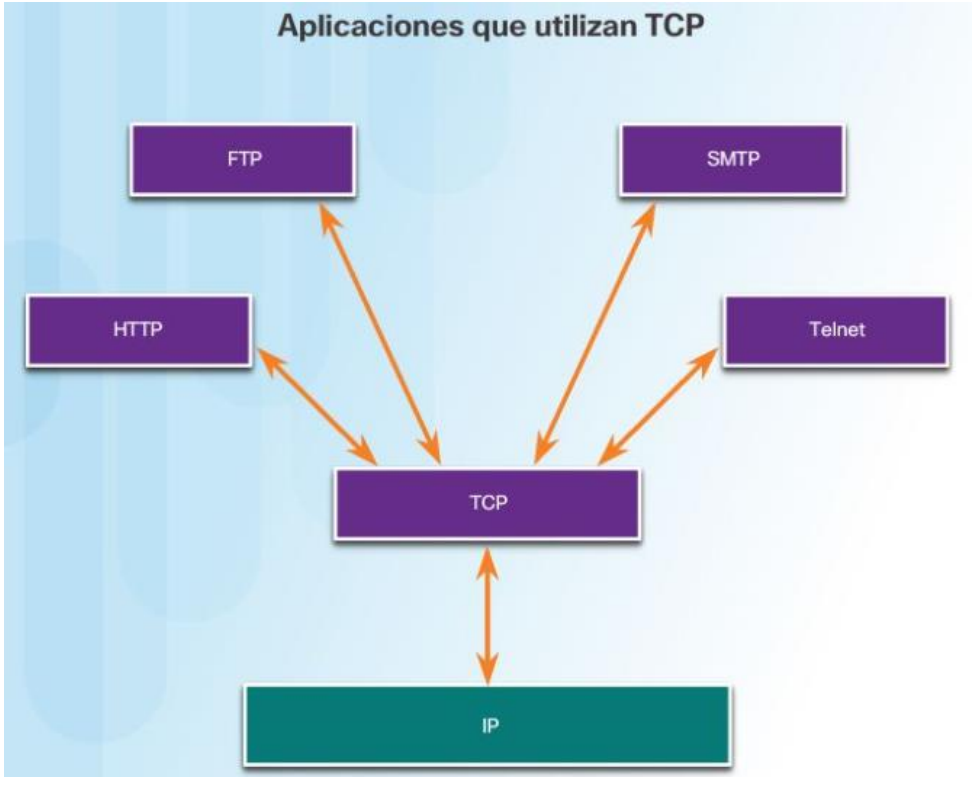
La tabla identifica y describe los diez campos de un encabezado TCP.

CAMPOS DE ENCABEZADO TCP	DESCRIPCION
Puerto de origen	Campo de 16 bits utilizado para identificar la aplicación de origen por número de puerto
Puerto de destino	Campo de 16 bits utilizado para identificar la aplicación de destino por número de puerto
Numero de secuencia	Campo de 32 bits utilizado para reensamblar datos
Numero de reconocimiento	Campo de 32 bits utilizado para indicar que se han recibido datos y el siguiente byte esperado de la fuente
Longitud del encabezado	Campo de 4 bits conocido como “desplazamiento de datos” que indica la longitud del encabezado del segmento TCP
Reservado	Campo de 6 bits reservado para uso futuro
Bits de control	Campo de 6 bits que incluye códigos de bit que indican el propósito y la función del segmento TCP
Tamaño de ventana	Campo de 16 bits utilizado para indicar el numero de bytes que se pueden aceptar a la vez
Suma de Comprobación	Campo de 16 bits utilizado para verificar errores en el segmento de encabezado y datos
Urgente	Campo de 16 bits utilizado para indicar si los datos contenidos son urgentes

9.2.4 Aplicaciones que Utilizan TCP

TCP es un buen ejemplo de cómo las diferentes capas del conjunto de protocolos TCP/IP tienen roles específicos. TCP maneja todas las tareas asociadas con la división del flujo de datos en segmentos, proporcionando confiabilidad, controlando el flujo de datos y reordenando segmentos.

TCP libera a la aplicación de tener que administrar estas tareas. Las aplicaciones, como las que se muestran en la figura, simplemente envían el flujo de datos a la capa de transporte y utilizan los servicios de TCP.



9.2.5 Verifique su Comprensión - Descripción General de TCP

¿Qué protocolo de la capa de transporte garantiza la entrega confiable en el mismo orden?

ICMP	IP	TCP ☺←	UDP

¿Qué enunciado de encabezado TCP es verdadero?

Se compone de 4 campos en un encabezado de 8 bytes.	Se compone de 8 campos en un encabezado de 10 bytes.
Se compone de 10 campos en un encabezado de 20 bytes. ☺←	Se compone de 20 campos en un encabezado de 40 bytes.

El encabezado TCP consta de 10 campos en un encabezado de 20 bytes.

¿Qué dos aplicaciones usarían el protocolo de capa de transporte TCP? (Elija dos opciones).

FTP ☺←	HTTP ☺←	ICMP	TFTP	VoIP

3. Descripción general de UDP

9.3.1 Características de UDP

Este tema abarcará UDP, lo que hace y cuándo es una buena idea usarlo en lugar de TCP. UDP es un ***protocolo de transporte del mejor esfuerzo***. UDP es un protocolo de transporte liviano que ofrece la misma segmentación y rearmado de datos que TCP, pero sin la confiabilidad y el control del flujo de TCP. UDP es un protocolo tan simple que se lo describe en términos de lo que no hace en comparación con TCP.

Las características UDP incluyen lo siguiente:

- Los datos se reconstruyen en el orden en que se recibieron.
- Los segmentos perdidos no se vuelven a enviar.
- No hay establecimiento de sesión.
- El envío no está informado sobre la disponibilidad de recursos.

Para obtener más información sobre UDP, busque en Internet el RFC.

9.3.2 El Encabezado UDP

UDP es un ***protocolo sin estado***, lo que significa que ni el cliente ni el servidor rastrean el estado de la sesión de comunicación. Si se requiere confiabilidad al utilizar UDP como protocolo de transporte, lo debe administrar la aplicación.

Uno de los requisitos más importantes para transmitir vídeo en vivo y voz a través de la red es que los datos fluyan rápidamente. Las aplicaciones de vídeo y de voz en vivo pueden tolerar cierta pérdida de datos con un efecto mínimo o imperceptible, y se adaptan perfectamente a UDP.

Los bloques de comunicación en UDP se denominan ***datagramas o segmentos***. Estos datagramas se envían con el mejor esfuerzo por el protocolo de la capa de transporte. El encabezado UDP es mucho más simple que el encabezado TCP porque solo tiene cuatro campos y requiere 8 bytes (64 bits). La figura muestra los campos en un encabezado TCP.

9.3.3 Campos del Encabezado UDP

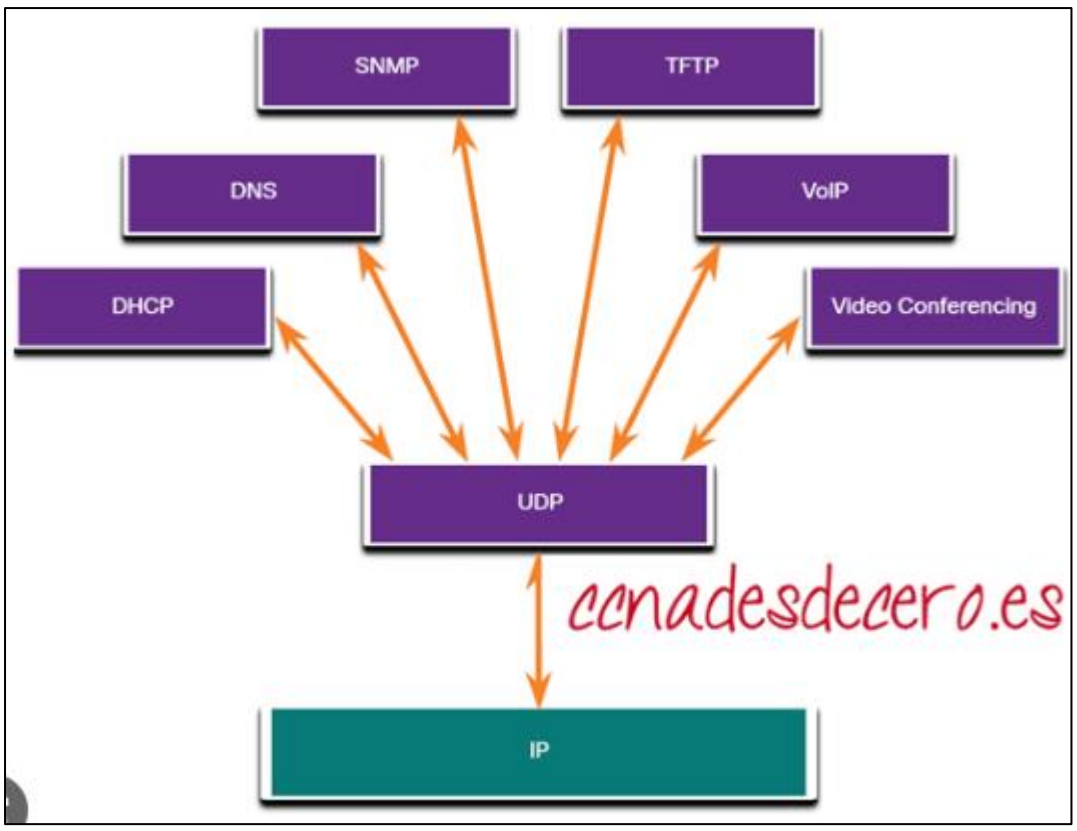
Campo de encabezado UDP	Descripción
Puerto de Origen	Campo de 16 bits utilizado para identificar la aplicación de origen por número de puerto
Puerto de destino	Campo de 16 bits utilizado para identificar la aplicación de destino por número de puerto
Duración	Campo de 16 bits que indica la longitud del encabezado del datagrama UDP
Suma de comprobación	Campo de 16 bits utilizado para la comprobación de errores del encabezado y datos del datagrama

9.3.4 Aplicaciones que Utilizan UDP

Existen tres tipos de aplicaciones que son las más adecuadas para UDP:

- **Aplicaciones de video en vivo y multimedia** - Estas aplicaciones pueden tolerar cierta pérdida de datos, pero requieren poco o ningún retraso. Los ejemplos incluyen VoIP y la transmisión de video en vivo.
- **Aplicaciones simples de solicitud y respuesta** - Aplicaciones con transacciones simples en las que un host envía una solicitud y puede o no recibir una respuesta. Los ejemplos incluyen DNS y DHCP.
- **Aplicaciones que manejan la confiabilidad por sí mismas** - Comunicaciones unidireccionales donde el control de flujo, la detección de errores, los reconocimientos y la recuperación de errores no son necesarios o la aplicación puede manejarlos. Los ejemplos incluyen los protocolos de la capa Aplicación: Simple Network Management Protocol (SNMP) y Trivial File Transfer Protocol (TFTP).

La figura identifica las aplicaciones que utilizan UDP.



Aunque DNS y SNMP utilizan UDP de manera predeterminada, ambos también pueden utilizar TCP. DNS utilizará TCP si la solicitud de DNS o la respuesta de DNS son más de 512 bytes, como cuando una respuesta de DNS incluye muchas resoluciones de nombre. Del mismo modo, en algunas situaciones, el administrador de redes puede querer configurar SNMP para utilizar TCP.

9.3.5 Verifique su Comprensión - Descripción General de UDP

¿Cuál de los siguientes es un protocolo de nivel de transporte de entrega sin estado?

ICMP	IP	TCP	UDP ☺←

¿Qué declaración de encabezado UDP es verdadera?

Se compone de 4 campos en un encabezado de 8 bytes. ☺←	Se compone de 8 campos en un encabezado de 10 bytes.
Se compone de 10 campos en un encabezado de 20 bytes.	Se compone de 20 campos en un encabezado de 40 bytes.

¿Qué dos aplicaciones usarían el protocolo de capa de transporte UDP? (Escoja dos opciones).

FTP	HTTP	ICMP	TFTP ☺←	VoIP ☺←

¿Qué dos campos son los mismos en un encabezado TCP y UDP? (Escoja dos opciones).

Bits de control	Número de puerto de destino ☺←
Número de secuencia	Número de puerto de origen ☺←
Número de puerto conocido	

4. Números de Puerto

9.4.1 Comunicaciones Separadas Múltiples

Como ha aprendido, hay algunas situaciones en las que TCP es el protocolo correcto para el trabajo, y otras situaciones en las que se debe usar UDP. Independientemente del tipo de datos que se transporten, tanto TCP como UDP utilizan ***números de puerto***.

Los protocolos de la capa Transporte TCP y UDP utilizan números de puerto para administrar múltiples conversaciones simultáneas. Como se muestra en la figura, los campos de encabezado TCP y UDP identifican un número de puerto de aplicación de origen y destino.

Puerto de origen (16)	Puerto de destino (16)

El número de puerto de origen está asociado con la aplicación de origen en el host local, mientras que el número de puerto de destino está asociado con la aplicación de destino en el host remoto. Por ejemplo, supongamos que un host está iniciando una solicitud de página web a un servidor web. Cuando el host inicia la solicitud de página web, genera dinámicamente el número de puerto de origen para identificar de forma exclusiva la conversación. Cada solicitud generada por un host utilizará un número de puerto de origen diferente creado dinámicamente. Este proceso permite establecer varias conversaciones simultáneamente.

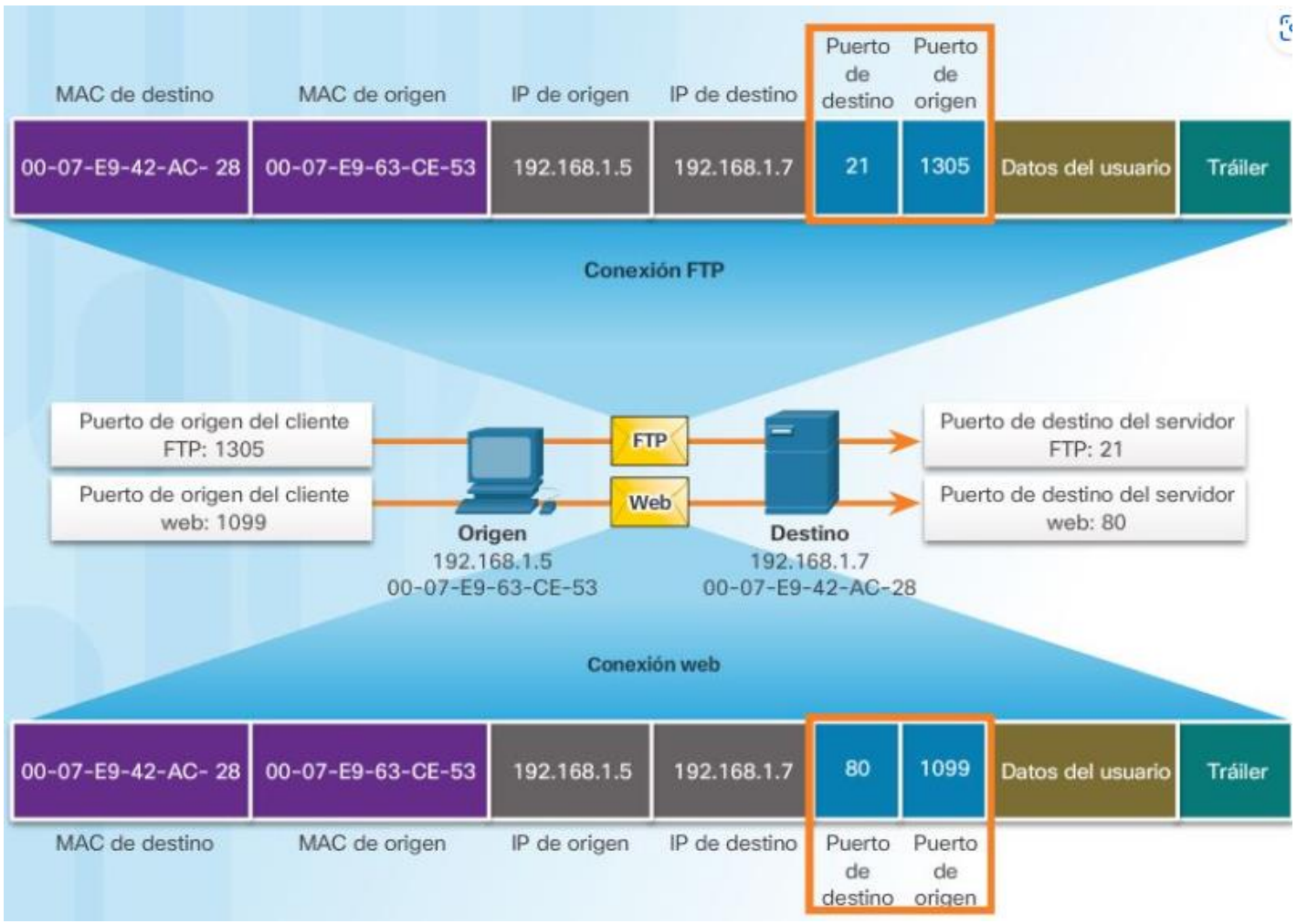
En la solicitud, el número de puerto de destino identifica el tipo de servicio que se solicita al servidor web destino. Por ejemplo, cuando un cliente especifica el ***puerto 80*** como puerto de destino, el servidor que recibe el mensaje sabe que se solicitan servicios web.

Un servidor puede ofrecer más de un servicio simultáneamente, como servicios web en el puerto 80, mientras que ofrece el establecimiento de conexión de Protocolo de Transferencia de Archivos (FTP) en el ***puerto 21***.

9.4.2 Pares de Sockets

Los puertos de origen y de destino se colocan dentro del segmento. Los segmentos se encapsulan dentro de un paquete IP. El paquete IP contiene la dirección IP de origen y de destino. Se conoce como ***socket*** a la combinación ***dirección IP de origen : número de puerto de origen***, o la combinación ***dirección IP de destino : número de puerto de destino***.

En el ejemplo de la figura, el PC está solicitando simultáneamente servicios FTP y web desde el servidor de destino.



En el ejemplo, la solicitud FTP generada por el PC incluye las direcciones MAC de Capa 2 y las direcciones IP de Capa 3. La solicitud también identifica el puerto de origen 1305 (generado dinámicamente por el host) y el puerto de destino, identificando los servicios FTP en el puerto 21. El host también ha solicitado una página web del servidor utilizando las mismas direcciones de Capa 2 y Capa 3. Sin embargo, está utilizando el número de puerto de origen 1099 (generado dinámicamente por el host) y el puerto de destino que identifica el servicio web en el puerto 80.

Un socket de cliente puede ser parecido a esto, donde 1099 representa el número de puerto de origen: ***192.168.1.5 : 1099***.

El socket se utiliza también para identificar el servidor y el servicio que solicita el cliente. El socket en un servidor web puede ser ***192.168.1.7 : 80.***

Juntos, estos dos sockets se combinan para formar un par de sockets: ***192.168.1.5 : 1099 ; 192.168.1.7 : 80***

Los sockets permiten que los diversos procesos que se ejecutan en un cliente se distingan entre sí. También permiten la diferenciación de diferentes conexiones a un proceso de servidor.

El número de puerto de origen actúa como dirección de retorno para la aplicación que realiza la solicitud. La capa de transporte hace un seguimiento de este puerto y de la aplicación que generó la solicitud de manera que cuando se devuelva una respuesta, esta se envíe a la aplicación correcta.

9.4.3 Grupos de Números de Puerto

La Autoridad de Números Asignados en Internet (IANA) es la organización responsable de asignar varios estándares de direccionamiento, incluidos los números de puerto de 16 bits. Los 16 bits utilizados para identificar los números de puerto de origen y destino proporcionan un rango de puertos entre ***0 y 65535.***

La IANA ha dividido el rango de números en los siguientes tres grupos de puertos.

GRUPO DE PUERTOS	RANGO DE NÚMEROS	DESCRIPCION
Puertos notables o bien conocidos	**0 a 1,023**	Para aplicaciones como navegadores web, clientes de correo electrónico y clientes de acceso remoto. Los puertos bien conocidos definidos para aplicaciones comunes de servidor, permiten a los clientes identificar fácilmente el servicio asociado requerido.
Puertos registrados	**1,024 a 49,151**	Estos números de puerto son asignados a una entidad que los solicite para utilizarlos en procesos o aplicaciones específicas. Principalmente estos procesos son aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un numero de puerto conocido. Por ejemplo, Cisco ha registrado el puerto 1812 para su proceso de autenticación del servidor RADIUS.
Puertos Privados y/o Dinámicos	**49,152 a 65,535**	Estos puertos se conocen también como puertos efímeros. El sistema operativo del cliente asigna números de puerto dinámicamente cuando se inicia una conexión a un servicio. El puerto dinámico identifica la aplicación cliente durante la comunicación.

Nota: Algunos sistemas operativos cliente utilizan números de puerto registrados en lugar de números de puerto dinámicos para asignar los puertos de origen. La tabla muestra algunos números de puerto bien conocidos y sus aplicaciones asociadas.

NUMERO DE PUERTO	APLICACIÓN	PROTOCOLO
20	Protocolo de transferencia de archivos (FTP) – Datos	TCP
21	Protocolo de transferencia de archivos (FTP) – Control	TCP
22	Shell Seguro (SSH)	TCP
23	Telnet	TCP
25	Protocolo Simple de Transferencia de Correo (SMTP)	TCP
53	Servicio de Nombres de Dominio (DNS Domain Name Service)	UDP, TCP
67	Protocolo de Configuración Dinámica de Host (DHCP) – Servidor	UDP
68	Protocolo de Configuración Dinámica de Host (DHCP) – Cliente	UDP
69	Protocolo Trivial de Transferencia de Archivos (TFTP)	UDP
80	Protocolo de Transferencia de Hipertexto (HTTP)	TCP
110	Protocolo de Oficina de Correos versión 3 (POP3)	TCP
143	Protocolo de acceso a mensajes de Internet (IMAP)	TCP
161	Protocolo Simple de Administración de Redes (SNMP)	UDP
443	Protocolo Seguro de Transferencia de Hipertexto (HTTPS)	TCP

Algunas aplicaciones pueden utilizar TCP y UDP. Por ejemplo, DNS utiliza UDP cuando los clientes envían solicitudes a un servidor DNS. Sin embargo, la comunicación entre dos servidores DNS siempre usa TCP.

Busque en el sitio web de IANA el registro de puertos para ver la lista completa de números de puerto y aplicaciones asociadas.

9.4.4 El Comando netstat

Las conexiones TCP no identificadas pueden representar una importante amenaza a la seguridad. Pueden indicar que algo o alguien está conectado al host local. A veces es necesario conocer las conexiones TCP activas que están abiertas y en ejecución en el host de red. Netstat es una utilidad de red importante que puede usarse para verificar esas conexiones. Como se muestra a continuación, ingrese el comando ***netstat*** para enumerar los protocolos en uso, la dirección local y los números de puerto, la dirección externas y los números de puerto, y el estado de la conexión.

De forma predeterminada, el comando **netstat** intentará resolver las direcciones IP en nombres de dominio y los números de puerto en aplicaciones conocidas. La opción **-n** se puede utilizar para mostrar direcciones IP y números de puerto en su formato numérico.

```
C:\> netstat

Active Connections

  Proto    Local Address          Foreign Address          State
  TCP      192.168.1.124:3126     192.168.0.2:netbios-ssn  ESTABLISHED
  TCP      192.168.1.124:3158     207.138.126.152:http     ESTABLISHED
  TCP      192.168.1.124:3159     207.138.126.169:http     ESTABLISHED
  TCP      192.168.1.124:3160     207.138.126.169:http     ESTABLISHED
  TCP      192.168.1.124:3161     sc.msn.com:http          ESTABLISHED
  TCP      192.168.1.124:3166     www.cisco.com:http       ESTABLISHED
(output omitted)
C:\>
```

9.4.5 Verifique su Comprensión - Números de Puerto

Supongamos que un host con dirección IP 10.1.1.10 desea solicitar servicios web a un servidor en 10.1.1.254. ¿Cuál de los siguientes mostraría el par de sockets correcto?

1099:10 .1.1.10, 80:10 .1.1.254	10.1.1. 10:80, 10.1.1. 254:1099
10.1.1. 10:1099, 10.1.1. 254:80 ☺←	80:10 .1.1.10, 1099:10 .1.1.254

¿Qué grupo de puertos incluye números de puerto para aplicaciones FTP, HTTP y TFTP?

puertos dinámicos	puertos privados
puertos registrados	puertos conocidos ☺←

¿Qué comando de Windows mostrará los protocolos en uso, la dirección local y los números de puerto, la dirección externa y los números de puerto y el estado de la conexión?

ipconfig /all	ping
netstat ☺←	traceroute

5. Proceso de Comunicación TCP

9.5.1 Procesos del Servidor TCP

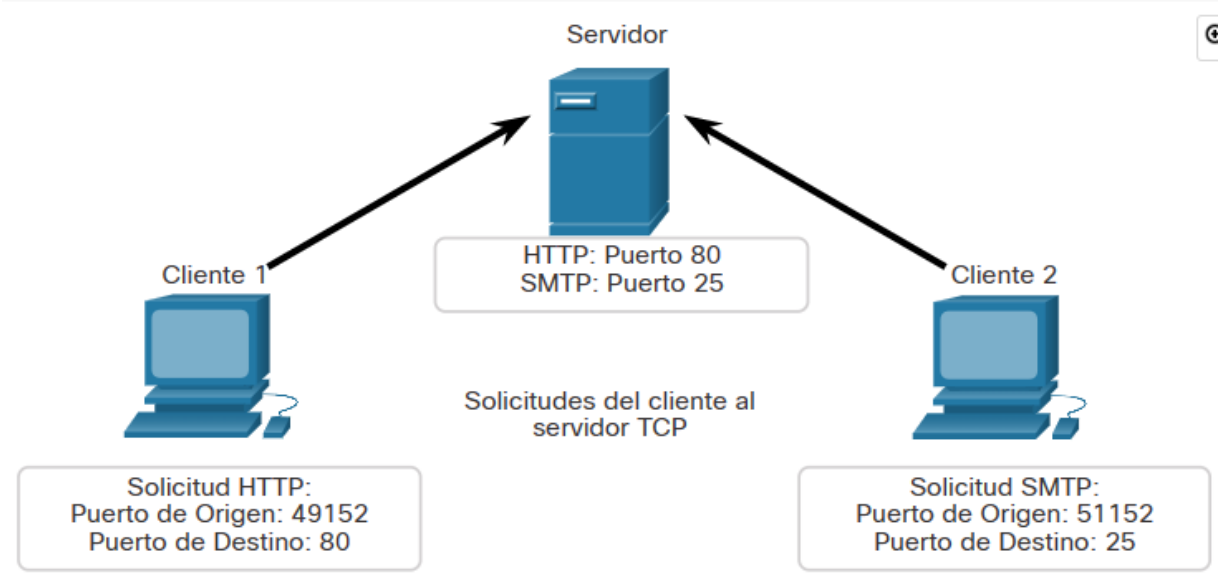
Ya conoce los fundamentos de TCP. Comprender el papel de los números de puerto le ayudará a comprender los detalles del proceso de comunicación TCP. En este tema, también aprenderá acerca de los procesos TCP de ***enlace de tres vías y terminación de sesión***.

Cada aplicación que se ejecuta en un servidor está configurada para utilizar un número de puerto. El número de puerto es asignado automáticamente o configurado manualmente por un administrador del sistema.

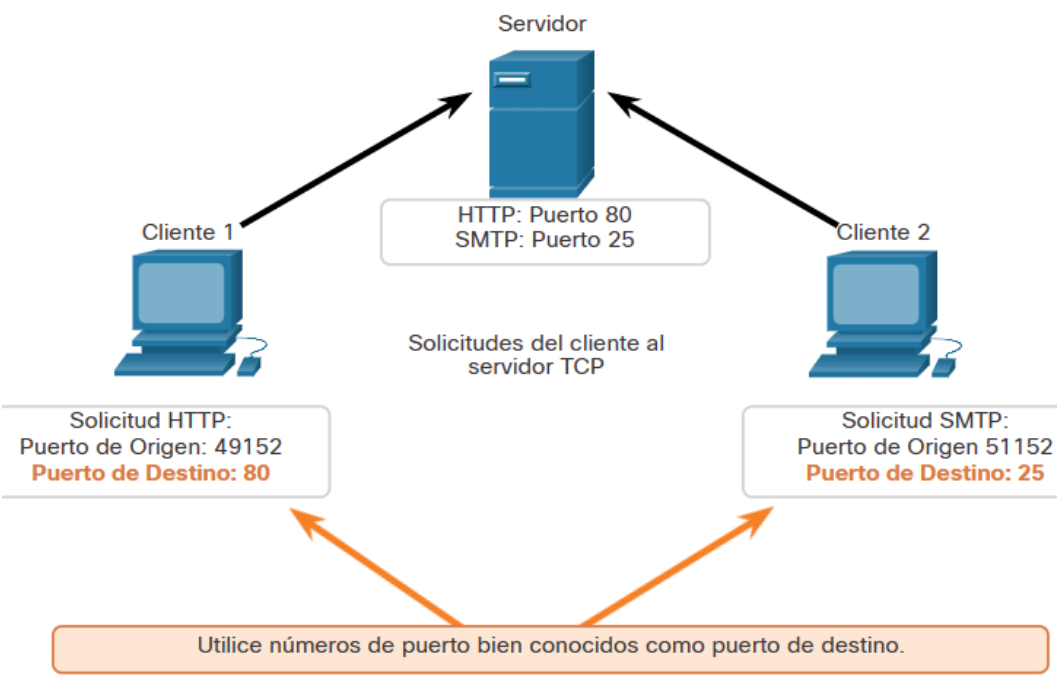
Un servidor individual no puede tener dos servicios asignados al mismo número de puerto dentro de los mismos servicios de la capa de transporte. Por ejemplo, un host que ejecuta una aplicación de servidor web y una aplicación de transferencia de archivos no puede tener ambos configurados para usar el mismo puerto, como el puerto TCP 80.

Una aplicación de servidor activa asignada a un puerto específico se considera abierta, lo que significa que la capa de transporte acepta y procesa los segmentos dirigidos a ese puerto. Toda solicitud entrante de un cliente direccionada al socket correcto es aceptada y los datos se envían a la aplicación del servidor. Pueden existir varios puertos abiertos simultáneamente en un servidor, uno para cada aplicación de servidor activa.

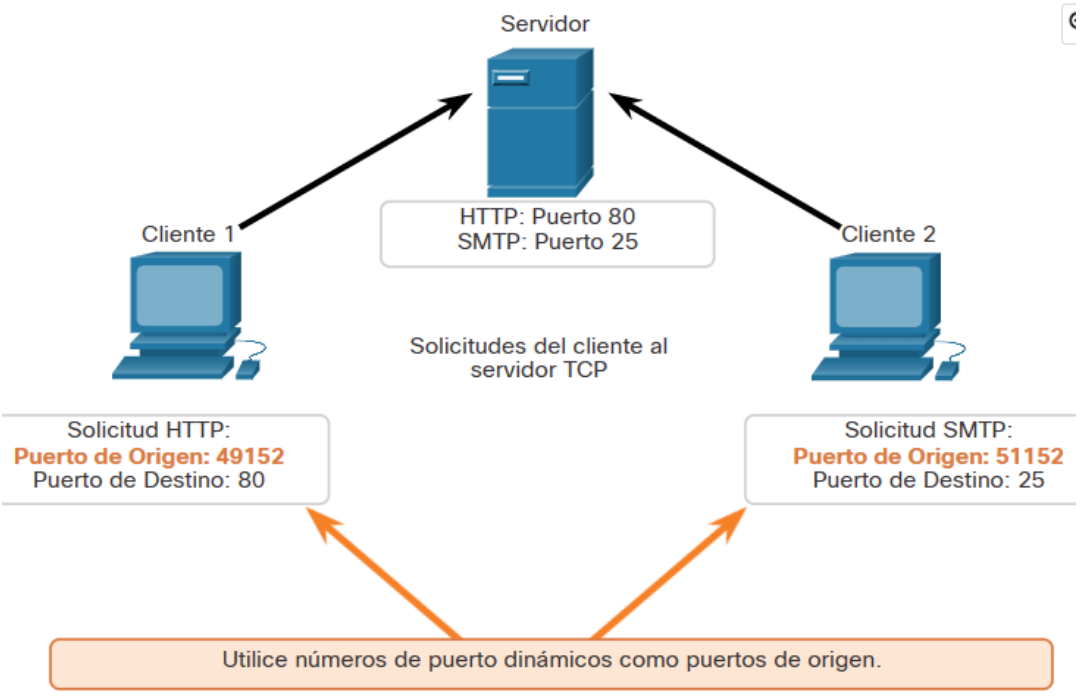
Clientes Enviando Solicitudes TCP
El Cliente 1 está solicitando servicios web y el Cliente 2 está solicitando servicio de correo electrónico del mismo servidor.



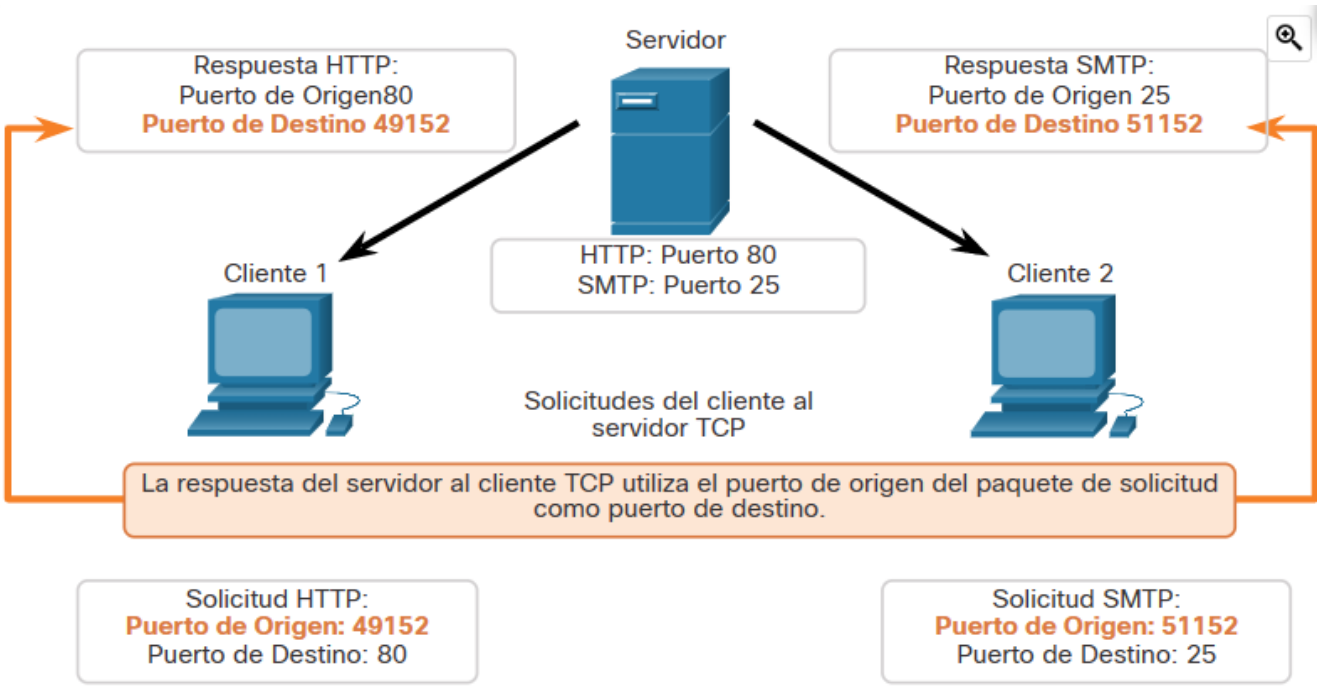
Puertos de Destino de la Solicitud
El cliente 1 está solicitando servicios web utilizando el conocido puerto de destino 80 (HTTP) y el cliente 2 está solicitando servicio de correo electrónico utilizando el conocido puerto de destino 25 (SMTP).



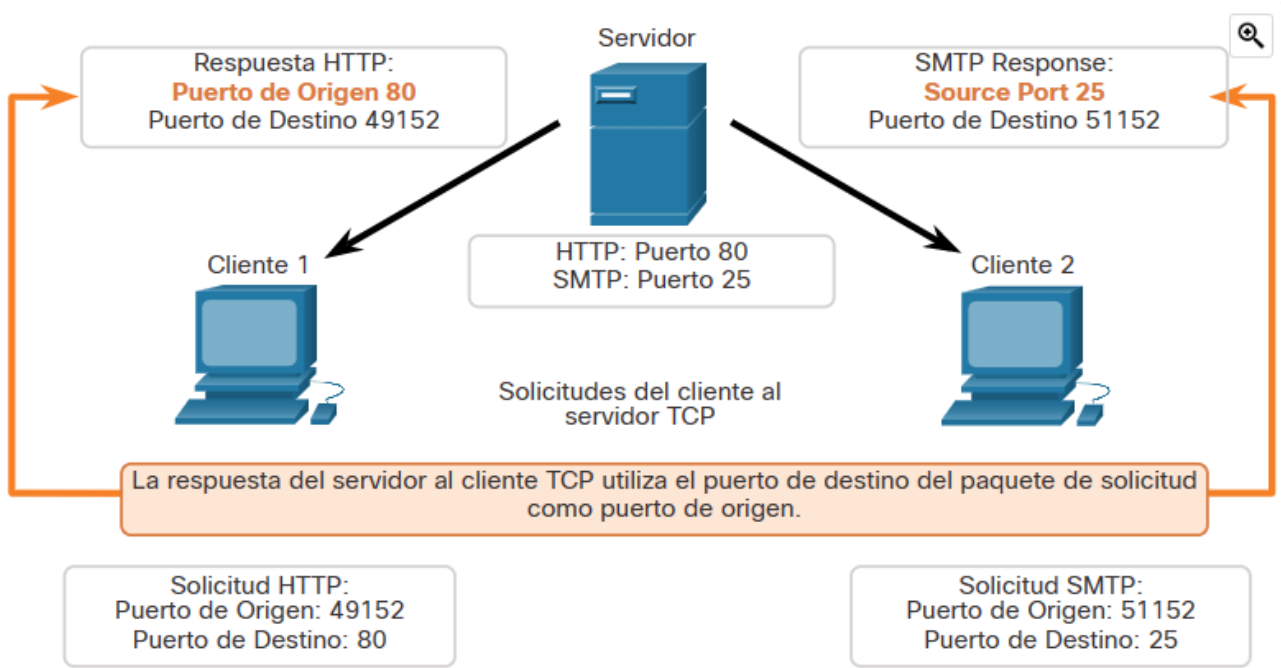
Puertos de Origen de Solicitud
Las solicitudes de cliente generan dinámicamente un número de puerto de origen. En este caso, el Cliente 1 está utilizando el puerto de origen 49152 y el Cliente 2 está utilizando el puerto de origen 51152.



Puertos Destino en la Respuesta
Cuando el servidor responde a las solicitudes del cliente, invierte los puertos de destino y origen de la solicitud inicial. Observe que la respuesta del servidor a la solicitud web ahora tiene el puerto de destino 49152 y la respuesta de correo electrónico ahora tiene el puerto de destino 51152.



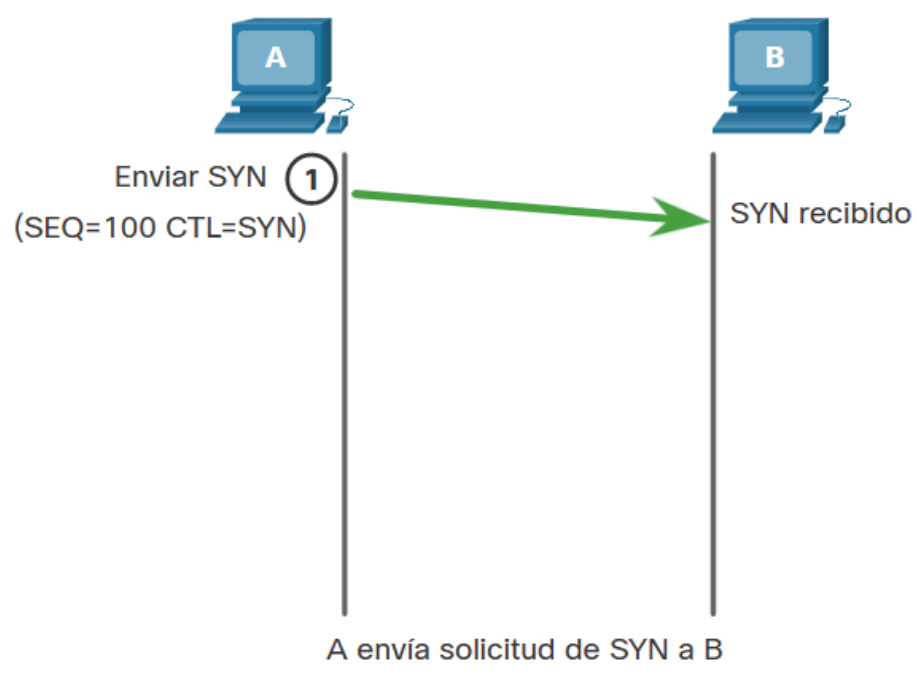
Puertos Origen en la Respuesta
El puerto de origen en la respuesta del servidor es el puerto de destino original en las solicitudes iniciales.



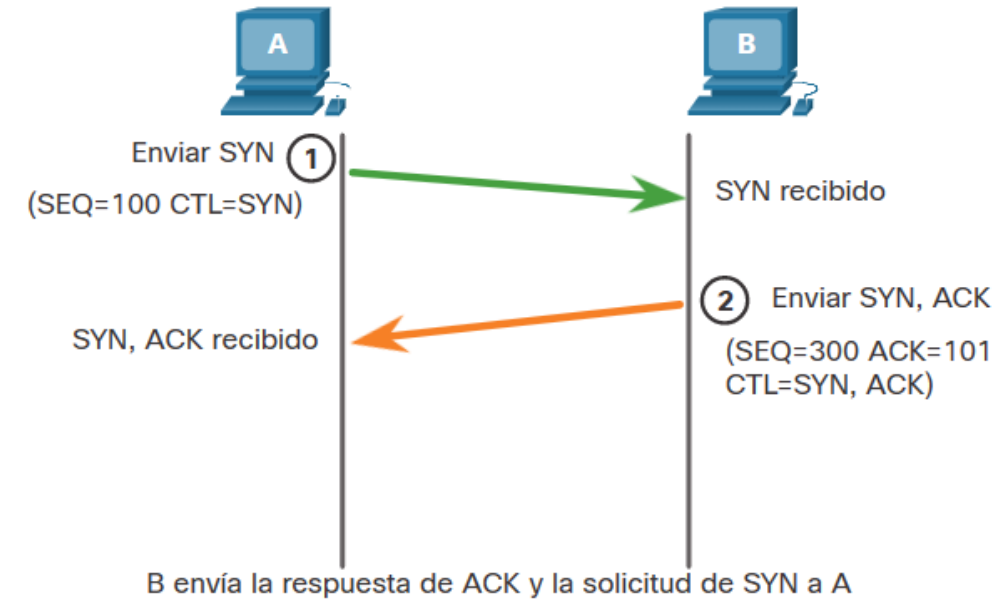
9.5.2 Establecimiento de Conexiones TCP

En algunas culturas, cuando dos personas se conocen, generalmente se saludan dándose la mano. Ambas partes entienden el acto de estrechar la mano como una señal de saludo amistoso. Las conexiones en la red son similares. En las conexiones TCP, el cliente establece la conexión con el servidor mediante el ***proceso de enlace de tres pasos o tres vías***.

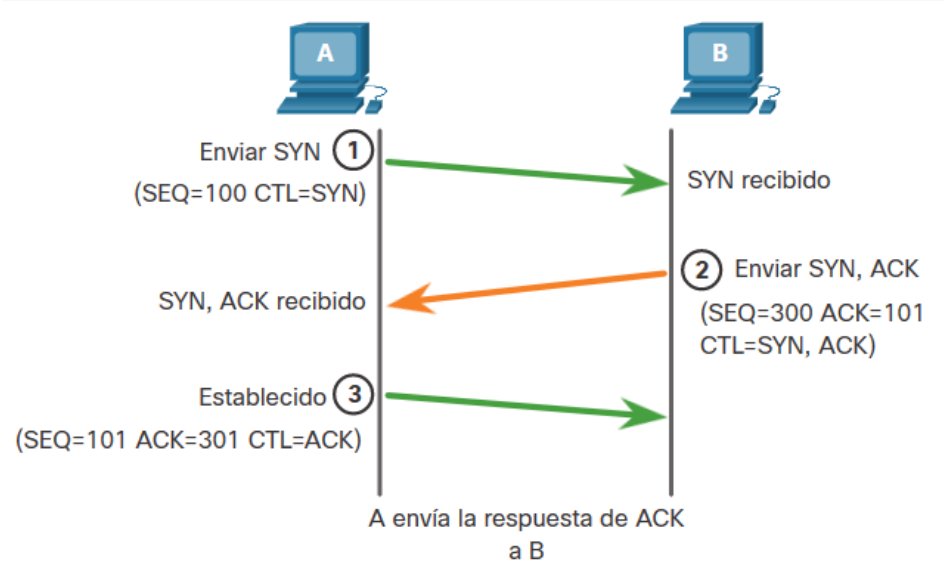
Paso 1. SOLICITUD SYN (synchronize= sincronizar)
El cliente de origen solicita una sesión de comunicación con el servidor.



Paso 2. ACK y SYN
El servidor acusa recibo (ACK= ACKNOWLEDGEMENT) de la comunicación cliente a servidor y solicita (SYN) una sesión de comunicación de servidor a cliente.



Paso 3. ACK
El cliente de origen acusa recibo de la sesión de comunicación de servidor a cliente.



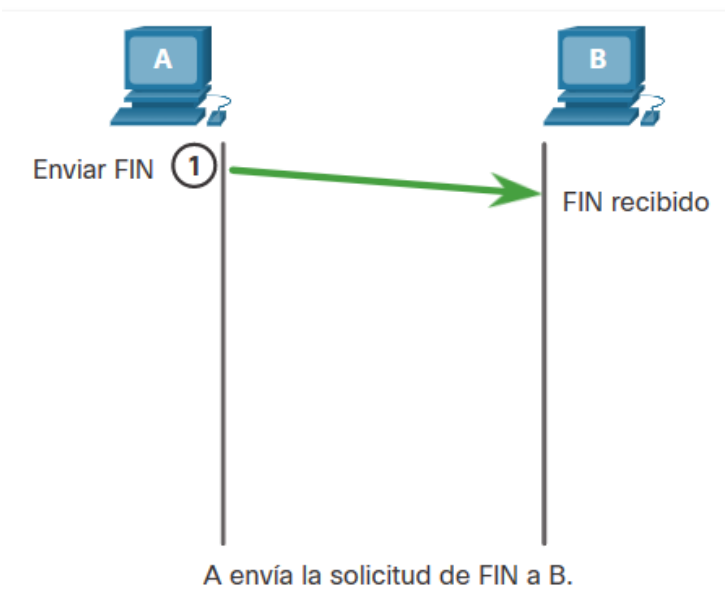
El protocolo de enlace de tres vías valida que el host de destino esté disponible para comunicarse. En este ejemplo, el host A ha validado que el host B está disponible.

9.5.3 Terminación de la Sesión

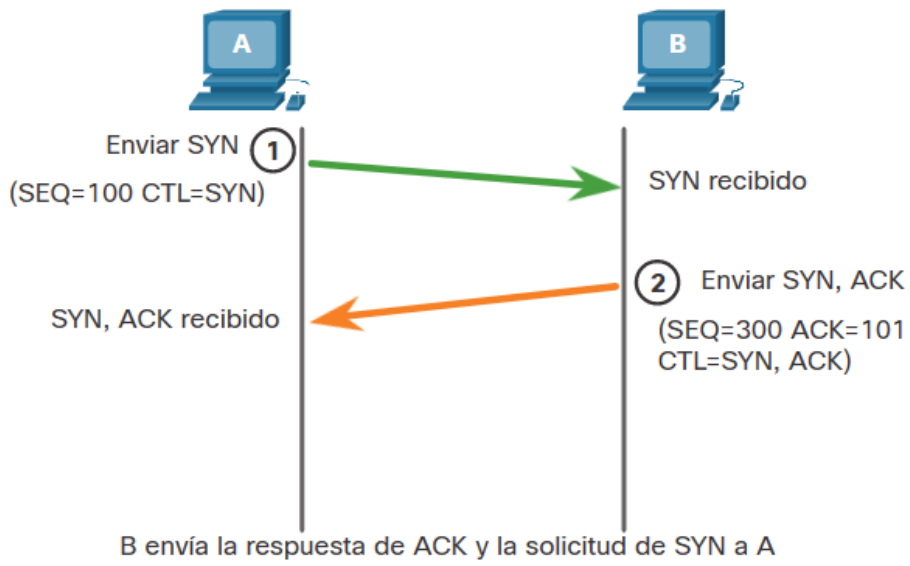
Para cerrar una conexión, se debe establecer el marcador de control de finalización (FIN) en el encabezado del segmento. Para finalizar todas las sesiones TCP simples, se utiliza un enlace de dos vías, que consta de un segmento FIN y un segmento de reconocimiento (ACK). Por lo tanto, para terminar una conversación simple admitida por TCP, se requieren cuatro intercambios para finalizar ambas sesiones. El cliente o el servidor pueden iniciar la terminación.

En el ejemplo, los términos cliente y servidor se utilizan como referencia por simplicidad, pero dos hosts que tengan una sesión abierta pueden iniciar el proceso de finalización.

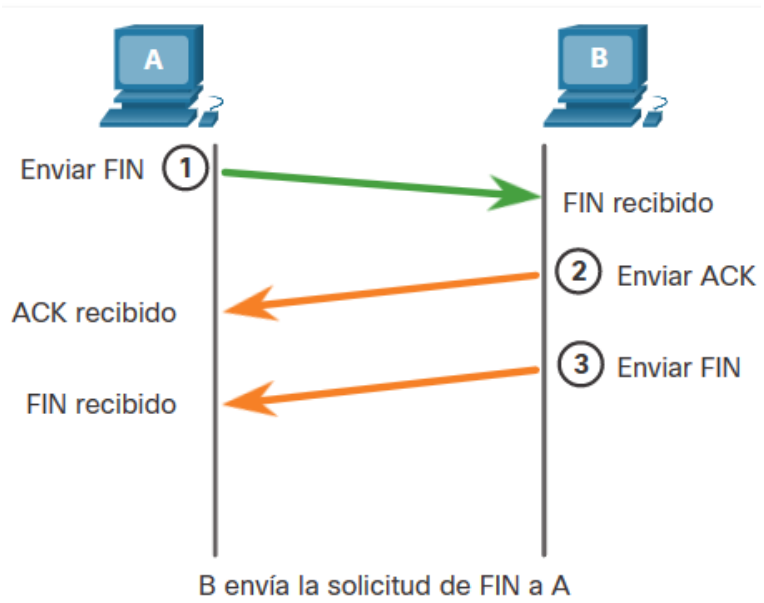
Paso 1. FIN
Cuando el cliente no tiene más datos para enviar en la transmisión, envía un segmento con el indicador FIN establecido.



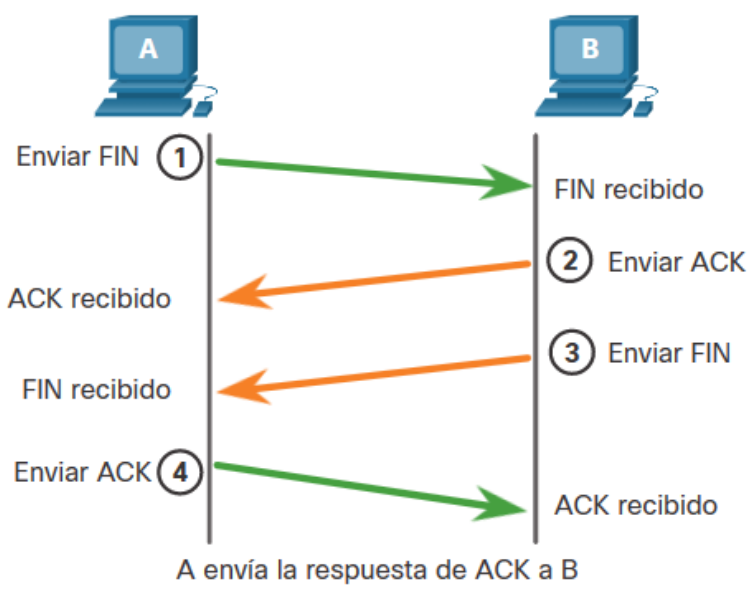
Paso 2. ACK
El servidor envía un ACK para acusar recibo del FIN para terminar la sesión de cliente a servidor.



Paso 3. FIN
El servidor envía un FIN al cliente para terminar la sesión de servidor a cliente.



Paso 4. ACK
El cliente responde con un ACK para dar acuse de recibo del FIN desde el servidor.



Una vez reconocidos todos los segmentos, la sesión se cierra.

9.5.4 Análisis del Protocolo TCP de Enlace de Tres Vías

Los hosts mantienen el estado, rastrean cada segmento de datos dentro de una sesión e intercambian información sobre qué datos se reciben utilizando la información en el encabezado TCP. TCP es un ***protocolo full-dúplex***, donde cada conexión representa dos sesiones de comunicación unidireccionales. Para establecer la conexión, los hosts realizan un enlace de tres vías. Como se muestra en la figura, los bits de control en el encabezado TCP indican el progreso y el estado de la conexión. Estas son las funciones del ***apretón de manos de tres vías***:

- Establece que el dispositivo de destino está presente en la red.
- Verifica que el dispositivo de destino tenga un servicio activo y acepte solicitudes en el número de puerto de destino que el cliente de origen desea utilizar.
- Informa al dispositivo de destino que el cliente de origen intenta establecer una sesión de comunicación en dicho número de puerto.

Una vez que se completa la comunicación, se cierran las sesiones y se finaliza la conexión. Los mecanismos de conexión y sesión habilitan la función de confiabilidad de TCP.

Campo de Bits de Control

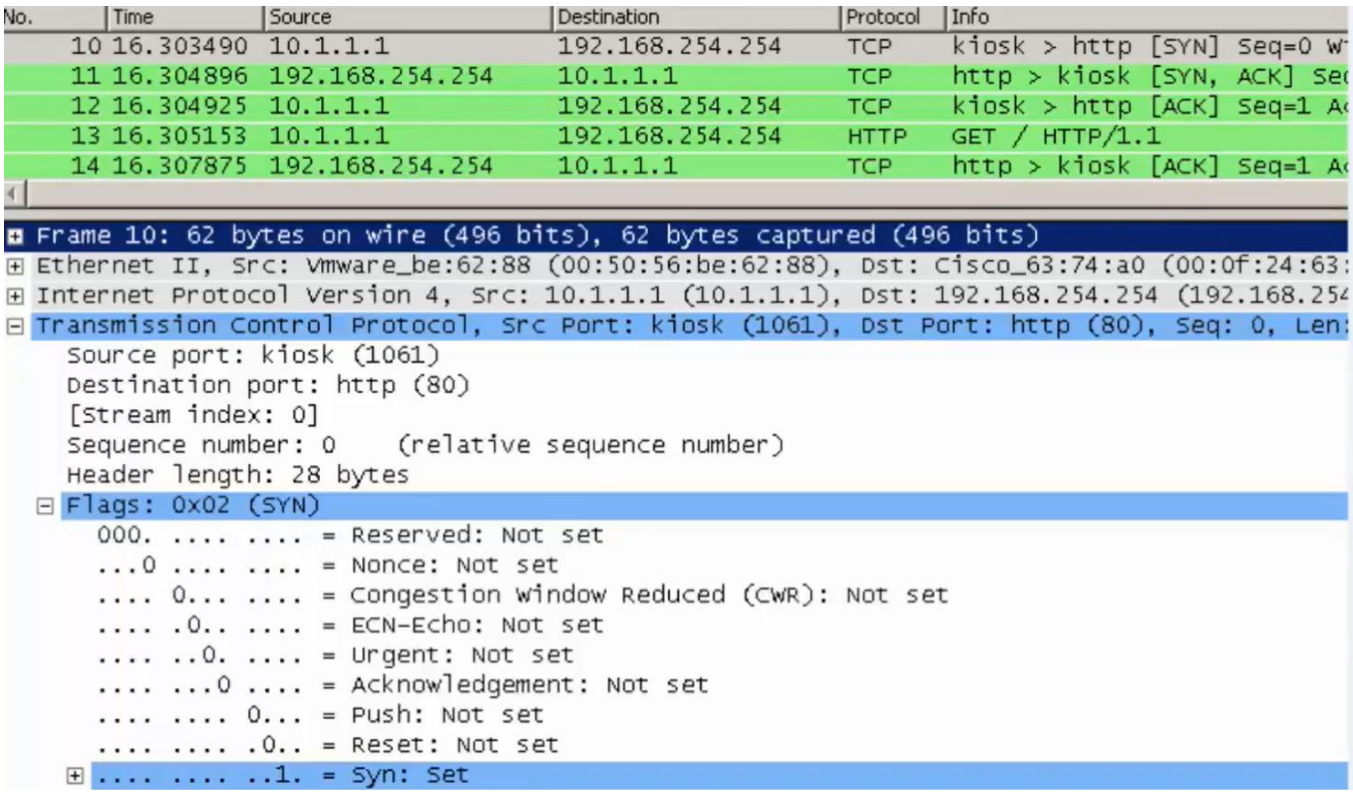
Los seis bits del campo ***Bits de Control*** del encabezado del segmento TCP también se conocen como ***marcadores***. Una bandera es un bit activado o desactivado (0 o 1). Los seis indicadores de bits de control son los siguientes:

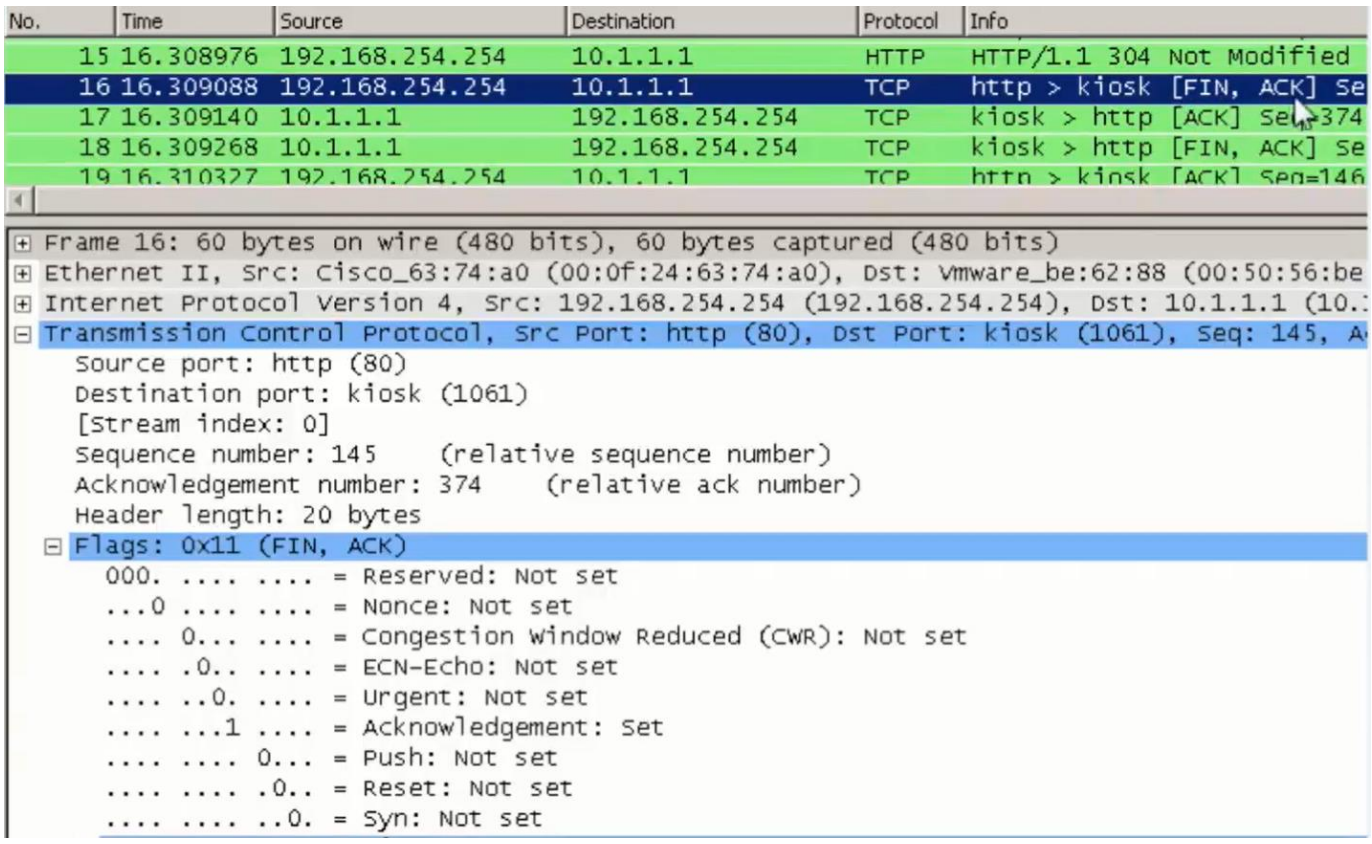
- **URG** - Indicador urgente
- **ACK**- Indicador de acuse de recibo utilizado en el establecimiento de la conexión y la terminación de la sesión
- **PSH** - Función de empuje
- **RST**- Restablece la conexión cuando se produce un error o un tiempo de espera
- **SYN**- Sincroniza números de secuencia utilizados en el establecimiento de conexión
- **FIN**- No más datos del remitente, se utiliza en la terminación de la sesión

Busque en Internet para obtener más información sobre las banderas ***PSH y URG***.

9.5.5 Video - Protocolo TCP de Enlace de 3 Vías

Tengo algunas capturas de pantalla de una captura de paquete de Wireshark que muestra el proceso de un protocolo de enlace TCP de 3 vías y la terminación de una conversación TCP. Analicemos estas capturas de pantalla para tener una idea de cómo funciona. TCP es un protocolo orientado a la conexión, lo que significa que primero se debe establecer una conexión de extremo a extremo antes de que se puedan enviar o recibir datos. El protocolo de enlace de 3 vías TCP inicia esa conexión. Cuando la conexión finalmente debe terminar, por ejemplo, digamos que es una conexión a un servidor web y usted cierra el navegador web, la conexión finaliza con dos enlaces bidireccionales. Un enlace de 3 vías de TCP involucra tres pasos: un SYN, un SYN y un ACK y un ACK. SYN significa sincronización, ACK significa reconocimiento. Primero, el host que inicia envía un segmento de sincronización SYN. El host que responde envía un reconocimiento ACK y su propio segmento de sincronización SYN, y luego el host inicial envía un segmento de reconocimiento ACK. De ahí el SYN, el SYN y ACK, y el ACK. Podemos ver que aquí en la parte superior de esta captura de pantalla, si miramos la ventana de Packet List, en los paquetes 10, 11 y 12, podemos ver un SYN, un SYN y un ACK, y un ACK. Este es el enlace de tres vías. Si observamos el paquete inicial en el enlace de tres vías, el segmento SYN aquí en la parte superior, podemos ver que el número de secuencia Seq=0. El comienzo del enlace de tres vías es un Seq=0 porque es el primer paquete en la conexión o conversación entre 2 hosts, o en este caso, entre un host y un servidor. El número de secuencia es un número aleatorio de 32 bits llamado ISN o número de secuencia inicial se elige aleatoriamente al principio de cada conversación TCP. Esto ayuda a protegerse contra los ataques de secuestro de TCP. Wireshark toma ese número aleatorio de 32 bits y lo convierte a cero, luego incrementa los números de secuencia SEQ y los ACK desde allí. Esto facilita la lectura, así como seguir los segmentos en orden usando el programa Wireshark. Veamos algunos de los detalles de este segmento inicial SYN. Bajamos a la ventana de detalles del paquete y podemos ver Sequence Number: 0, que es el número de secuencia relativo. Si miramos los Flags, vemos que el bit SYN: Set (se estableció). Lo puede ver aquí al lado del 1. En el siguiente paquete, el paquete #11, el servidor responde al segmento de sincronización inicial SYN. Iré a la siguiente captura de pantalla y ahora el paquete 11 está resaltado. El servidor responde con un ACK (acuse de recibo), reconociendo la Seq=0 y ACK=1, allí entonces, el Seq se incrementa a Seq=1 y el ACK=1 que fue enviado. Podemos ver en la ventana de detalles del protocolo el Acknowledgement Number=1 y que es el ACK relativo. El servidor también envió su propio segmento de sincronización SYN=0, es cero desde la conversación inicial en sentido contrario. Si miramos en la ventana de detalles, podemos ver que el Sequence Number=0, ese es un número de secuencia relativo del servidor al host. Si miramos aquí los Flags, tanto el bit SYN como ACK se han configurado. Si vamos a la siguiente captura de pantalla en el paquete 12, que es el paso tres en el protocolo de enlace de tres vías, el host 10.1.1.1 responde con un reconocimiento o ACK y si miramos en la ventana de detalles del protocolo, vemos que el número de reconocimiento es 1, es decir se ha incrementado en 1. Puede ver aquí que el bit de reconocimiento se ha establecido, pero observe que el bit SYN no se ha establecido. Esta es la fase final en el protocolo de enlace de tres vías. Ahora veamos cómo termina la conexión TCP. Iré a la siguiente captura de pantalla y pueden ver en el paquete 16 que el host envió al servidor un segmento con un final o Fin y un reconocimiento o ACK. En este segmento tenemos un FIN y un ACK, FIN es para terminar la conversación. El indicador de reconocimiento ACK se ha establecido por primera vez según el protocolo de enlace de tres vías, y en cada segmento enviado a partir de entonces, se establece el indicador de reconocimiento o acuse de recibo que reconoce que la conversación ha terminado. Puede ver que en el siguiente paquete 17, el host respondió al servidor con un acuse de recibo, que confirma que la conversación terminó. Este es un enlace de dos vías, un FIN un ACK y un ACK. Si miramos hacia adelante en la ventana de la lista de paquetes al paquete 18, puede ver que el host 10.1.1.1 envía luego al servidor su propio FIN y ACK, luego el servidor responde con su propio ACK. Así que tiene dos enlaces bidireccionales para terminar la conexión. Si vuelvo a la captura de pantalla anterior y miro los detalles del paquete 16, podemos ver aquí en el segmento TCP los FLAGS. Fíjate en el Acknowledgement y el FIN, ambos están en SET o configurados. Observe que Acknowledgement Number=374, lo que indica que estas capturas de pantalla probablemente se generaron a partir de dos capturas de paquetes independientes en Wireshark. Puedes ver en estas dos últimas capturas de pantalla cómo la conversación termina con dos enlaces bidireccionales, uno es (FIN,ACK) y ACK, y el otro enlace es en la otra dirección.





9.5.6 Verifique su Comprensión - Proceso de Comunicación TCP

¿Cuáles de los siguientes puertos serían válidos de origen y destino para un host que se conecta a un servidor de correo electrónico?

Origen: 25, Destino: 49152	Origen : 80, Destino: 49152
Origen: 49152, Destino: 25 ☺←	Origen: 49152, Destino: 80

El puerto de destino es el puerto conocido para Simple Mail Transport Protocol, que es 25. Este es el puerto en el que el servidor de correo estará escuchando. El cliente solicitante selecciona dinámicamente el puerto de origen y puede ser 49152.

¿Qué indicadores de bits de control se utilizan durante el apretón de manos de tres vías?

ACK y FIN	FIN y RESET
RESET y SIN	SYN y ACK ☺←

El protocolo de enlace de tres vías consta de tres intercambios de mensajes con los siguientes indicadores de bits de control: SYN, SYN ACK y ACK

¿Cuántos intercambios se necesitan para finalizar ambas sesiones entre dos hosts?

UNO	DOS	TRES	CUATRO ☺←	CINCO

Hay cuatro intercambios para finalizar ambas sesiones entre dos hosts. (1) El host A envía una FIN. (2) El host B envía un ACK. (3) El host B envía un FIN. (4) El host A envía un ACK.

6. Confiabilidad y Control de Flujo

9.6.1 Confiabilidad de TCP - Entrega Garantizada y Ordenada

La razón por la que TCP es el mejor protocolo para algunas aplicaciones es porque, a diferencia de UDP, reenvía paquetes descartados y paquetes numerados para indicar su orden correcto antes de la entrega. TCP también puede ayudar a mantener el flujo de paquetes para que los dispositivos no se sobrecarguen. En este tema se tratan detalladamente estas características de TCP.

Puede haber momentos en que los segmentos TCP no llegan a su destino. Otras veces, los segmentos TCP podrían llegar fuera de servicio. Para que el receptor comprenda el mensaje original, los datos en estos segmentos se vuelven a ensamblar en el orden original. Para lograr esto, se asignan números de secuencia en el encabezado de cada paquete. El número de secuencia representa el primer byte de datos del segmento TCP.

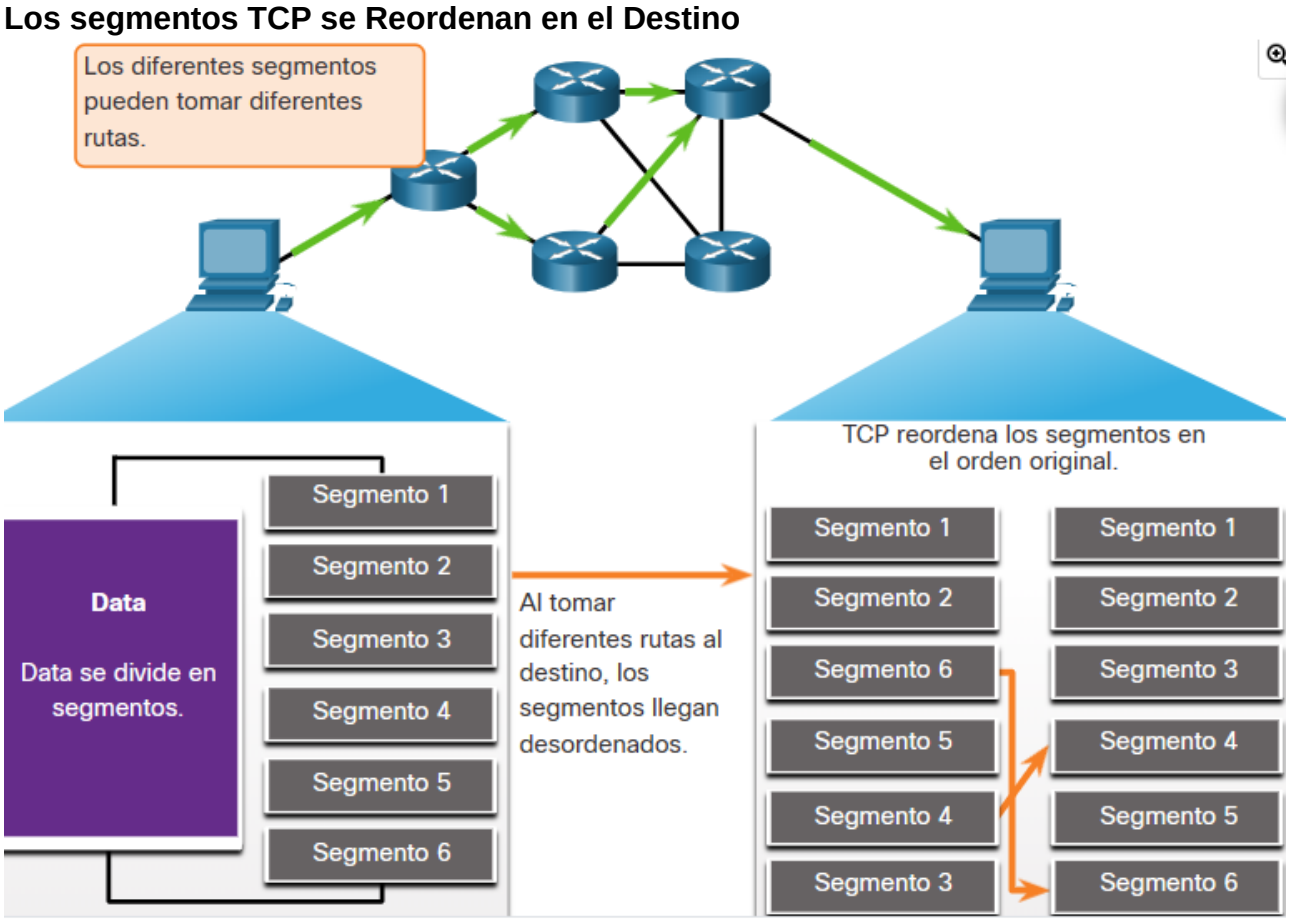
Durante la configuración de la sesión, se establece un ***ISN (Número de Secuencia Inicial)***. Este ISN representa el valor inicial de los bytes que se transmiten a la aplicación receptora. A medida que se transmiten los datos durante la sesión, el número de secuencia se incrementa según el

número de bytes que se han transmitido. Este seguimiento de bytes de datos permite identificar y reconocer cada segmento de manera exclusiva. A partir de esto, se pueden identificar segmentos perdidos.

El ISN no comienza en uno, pero es efectivamente un ***número aleatorio***. Esto permite evitar ciertos tipos de ataques maliciosos. Para mayor simplicidad, usaremos un ISN de 1 para los ejemplos de este módulo.

Los números de secuencia de segmento indican cómo reensamblar y reordenar los segmentos recibidos, como se muestra en la figura.

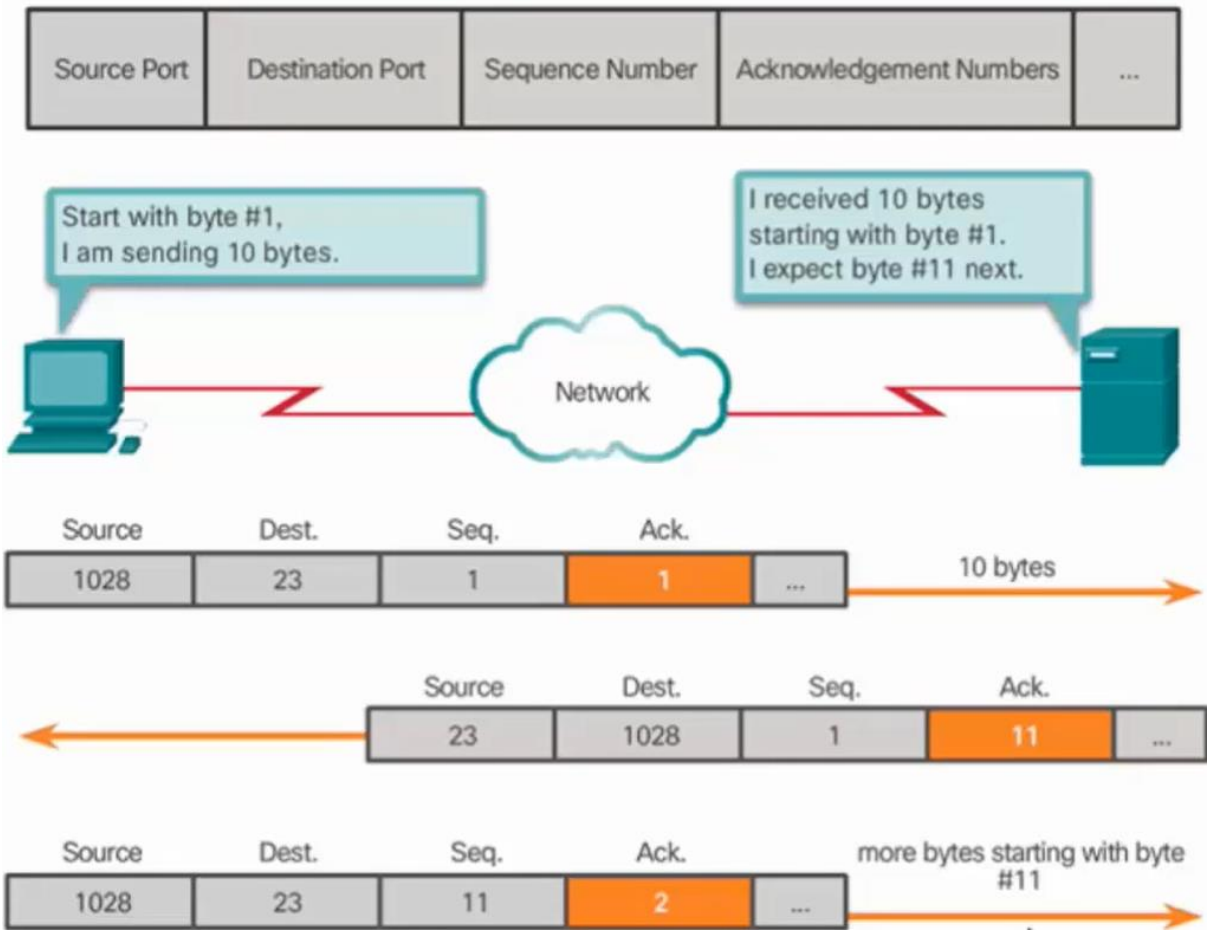
Los segmentos TCP se Reordenan en el Destino



El ***proceso TCP receptor*** coloca los datos del segmento en un búfer de recepción. Los segmentos se colocan en el orden de secuencia adecuado y se pasan a la capa Aplicación cuando se vuelven a montar. Todos los segmentos que lleguen con números de secuencia desordenados se retienen para su posterior procesamiento. A continuación, cuando llegan los segmentos con bytes faltantes, tales segmentos se procesan en orden.

9.6.2 Video - Confiabilidad de TCP - Números de Secuencia y Acuses de Recibo

Una de las funciones de TCP es garantizar que cada segmento llegue a su destino. Los servicios TCP en el host de destino reconocen los datos que ha recibido la aplicación de origen. Este video muestra un ejemplo simplificado de las operaciones de TCP y no es necesariamente una representación realista. TCP es un protocolo orientado a la conexión en el que primero se establece una conexión mediante el protocolo de enlace de tres vías antes de enviar los datos. Otra característica de TCP es que es un protocolo confiable. Dos cosas que lo hacen confiable son los números de secuencia y los acuses de recibo. Cada segmento TCP que se envía en una conversación TCP obtiene un número de secuencia, por lo que cada bit de datos se numera básicamente en una lista secuencial. Esto permite que el host receptor reconstruya los datos a partir de los segmentos numerados ordenados. Si los datos llegan desordenados al extremo receptor, los datos se pueden volver a juntar en el orden correcto gracias a los números de secuencia. Los reconocimientos entran en juego al ayudar al remitente saber que los datos que se envían en realidad se están recibiendo. La forma en que esto funciona es que el host emisor envía segmentos TCP en bytes, y el host receptor reconoce los bytes recibidos mediante el envío de confirmaciones ACK. Hay un límite en la cantidad de datos que el host emisor puede enviar antes de recibir un reconocimiento del receptor, esta cantidad se llama el ***tamaño de ventana***. El tamaño de ventana es la cantidad total de bytes enviados en segmentos TCP antes de recibir un reconocimiento. Mediante el escalado de ventana TCP las computadoras pueden alcanzar tamaños de ventana grandes de hasta 1 gigabyte. Entonces como el host emisor envía bytes de datos en segmentos TCP, el host receptor devuelve reconocimientos a medida que procesa los bytes recibidos y libera sus búferes. Podemos ver esto representado en este gráfico, comencemos leyendo el mensaje del host emisor aquí. Comience con el byte número uno, estoy enviando 10 bytes. En este escenario los 10 bytes son el tamaño de la ventana. En la realidad, el tamaño de la ventana es mucho mayor que 10 bytes, ya que hoy en día los tamaños de ventana suelen ser de 16 megabytes o más, pero esto funciona bien para este ejemplo. Entonces, el host envía 10 bytes comenzando con el byte número 1. El host receptor en este caso un servidor dice: “Recibí 10 bytes comenzando con el byte número uno, espero el siguiente byte 11”: Este es el acuse de recibo o reconocimiento. El servidor reconoce que recibió los 10 bytes y ahora espera el número 11. Si miramos aquí abajo, podemos ver en este segmento, comenzando con el número de secuencia 1, se han enviado 10 bytes. El receptor envía un ACK 11. Comenzando con numero de secuencia 1 se enviaron 10 bytes, por lo que el siguiente número de secuencia que se espera es un 11. Este reconocimiento se envía de regreso al host de origen. Ahora el host de origen envía 10 bytes más comenzando con el número de secuencia 11. Si tuviéramos que preguntarnos cuál sería el próximo ACK que el servidor enviaría de regreso al host de origen, tendríamos que preguntarnos cuál es el último número de secuencia enviado. Comenzando con 11 se enviaron 10 bytes, entonces el último número de secuencia enviado fue 20. Entonces, el ACK sería un 21. Ese es el siguiente número de secuencia esperado. Puede ver cómo los números de secuencia y los reconocimientos, incluido el tamaño de la ventana, hacen que TCP sea un protocolo muy ordenado y confiable.

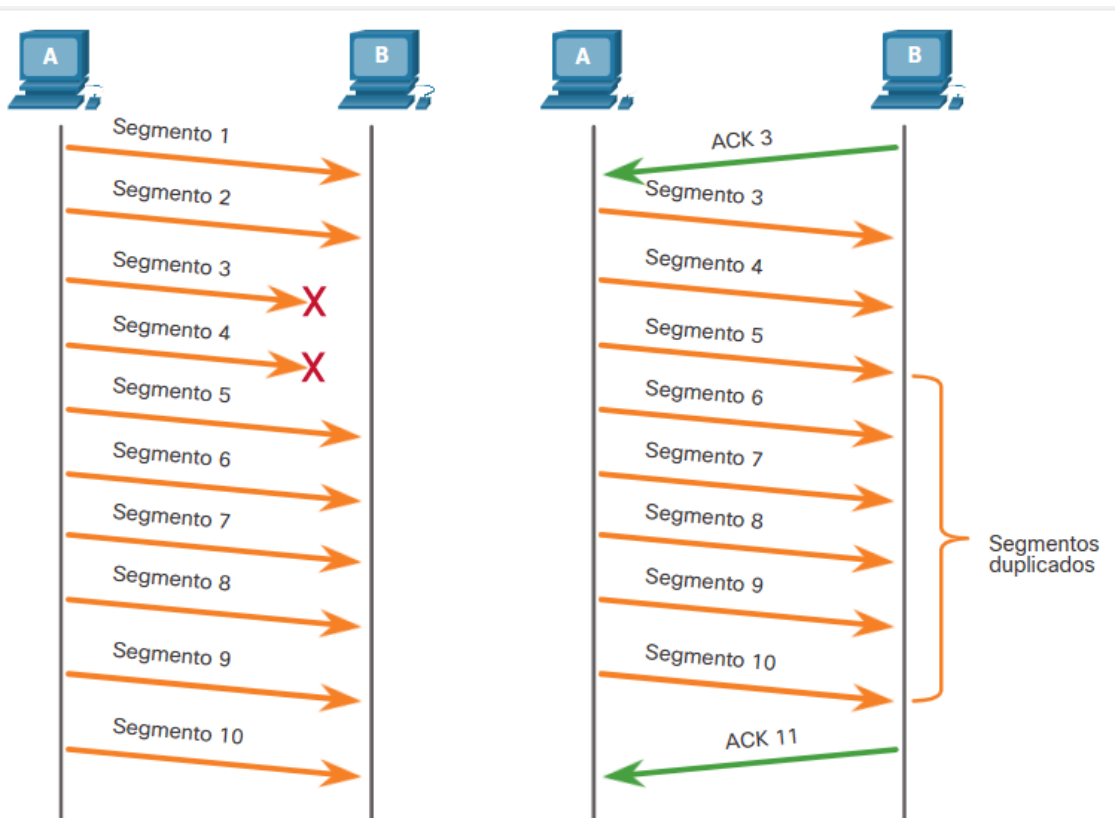


9.6.3 Confiabilidad de TCP - Pérdida de Datos y Retransmisión

No importa cuán bien diseñada esté una red, ocasionalmente se produce la pérdida de datos. TCP proporciona métodos para administrar la pérdida de segmentos. Entre estos está un mecanismo para retransmitir segmentos para los datos sin reconocimiento.

El número de secuencia (SEQ) y el número de acuse de recibo (ACK) se utilizan juntos para confirmar la recepción de los bytes de datos contenidos en los segmentos transmitidos. El número SEQ identifica el primer byte de datos en el segmento que se transmite. TCP utiliza el número ACK reenviado al origen para indicar el próximo byte que el receptor espera recibir. Esto se llama acuse de recibo de expectativa.

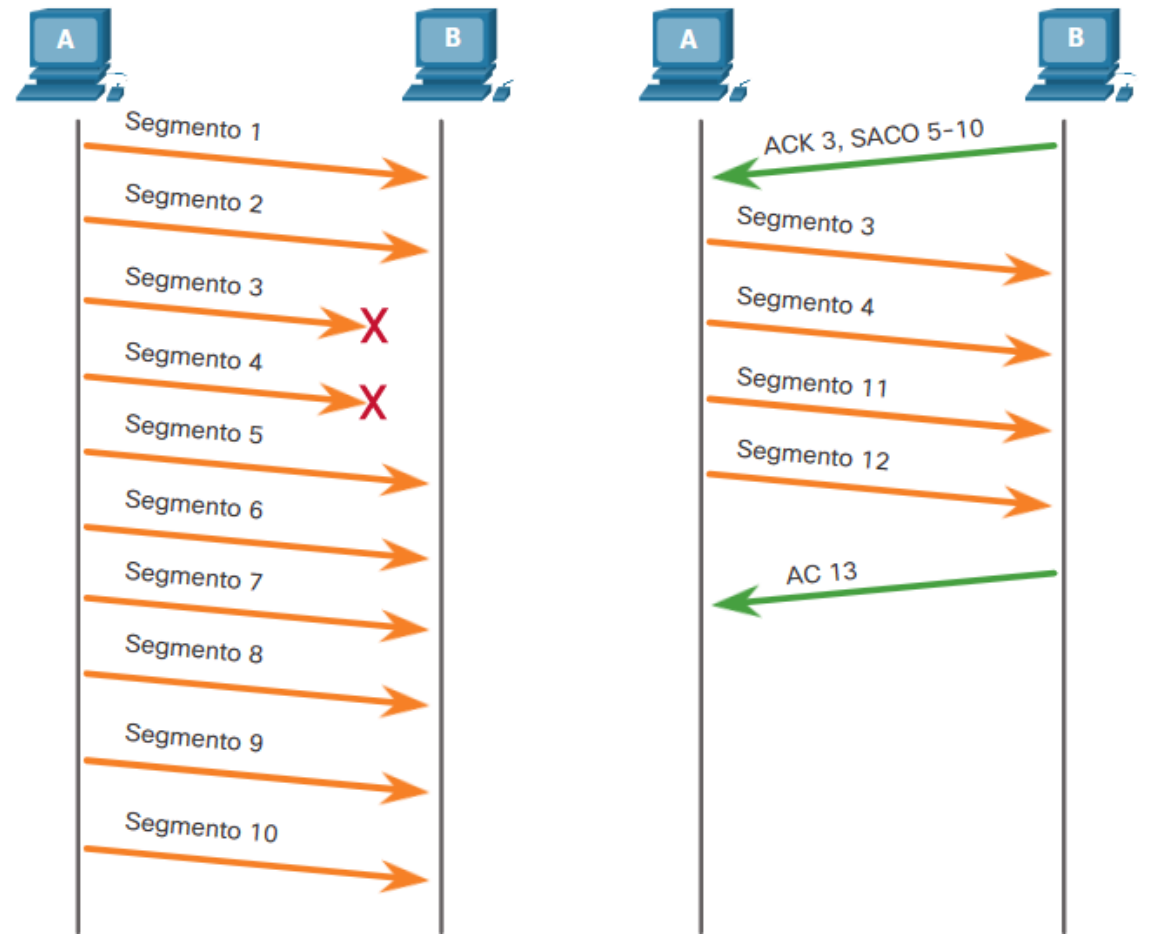
Antes de mejoras posteriores, TCP solo podía reconocer el siguiente byte esperado. Por ejemplo, en la figura, utilizando números de segmento para simplificar, el host A envía los segmentos del 1 al 10 al host B. Si llegan todos los segmentos excepto los segmentos 3 y 4, el host B respondería con acuse de recibo especificando que el siguiente segmento esperado es el segmento 3. El host A no tiene idea de si algún otro segmento llegó o no. Por lo tanto, el host A reenviaría los segmentos 3 a 10. Si todos los segmentos de reenvío llegan correctamente, los segmentos 5 a 10 serían duplicados. Esto puede provocar retrasos, congestión e ineficiencias.



Los sistemas operativos actualmente suelen emplear una característica TCP opcional llamada ***SACK (reconocimiento selectivo)***, negociada durante el protocolo de enlace de tres vías. Si ambos hosts admiten SACK, el receptor puede reconocer explícitamente qué segmentos (bytes) se recibieron, incluidos los segmentos discontinuos. Por lo tanto, el host emisor solo necesitaría retransmitir los datos faltantes. Por ejemplo, en la siguiente figura, utilizando de nuevo números de segmento para simplificar, el host A envía los segmentos 1 a 10 al host B. Si llegan todos los segmentos excepto los segmentos 3 y 4, el host B puede reconocer que ha recibido los segmentos 1 y 2 (ACK 3) y reconocer selectivamente los segmentos 5 a 10 (SACK 5-10). El host A solo necesitaría reenviar los segmentos 3 y 4.

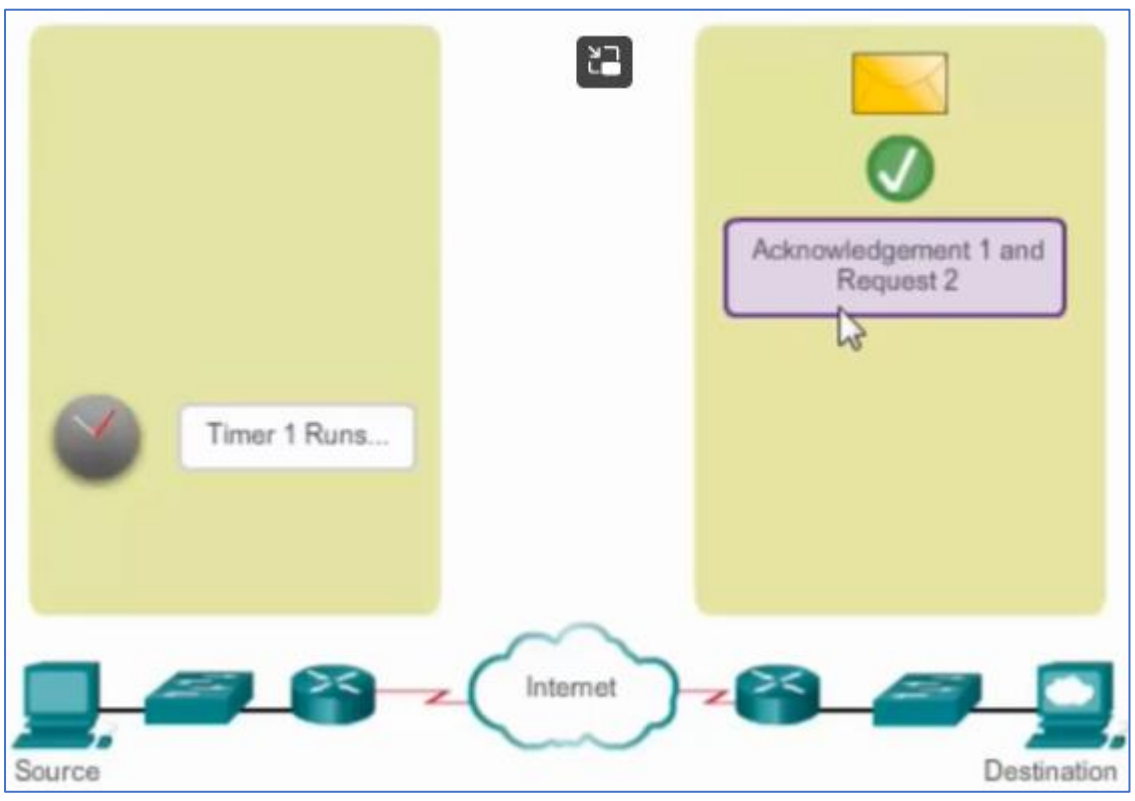
Nota: TCP normalmente envía ACK para cada otro paquete, pero otros factores más allá del alcance de este tema pueden alterar este comportamiento.

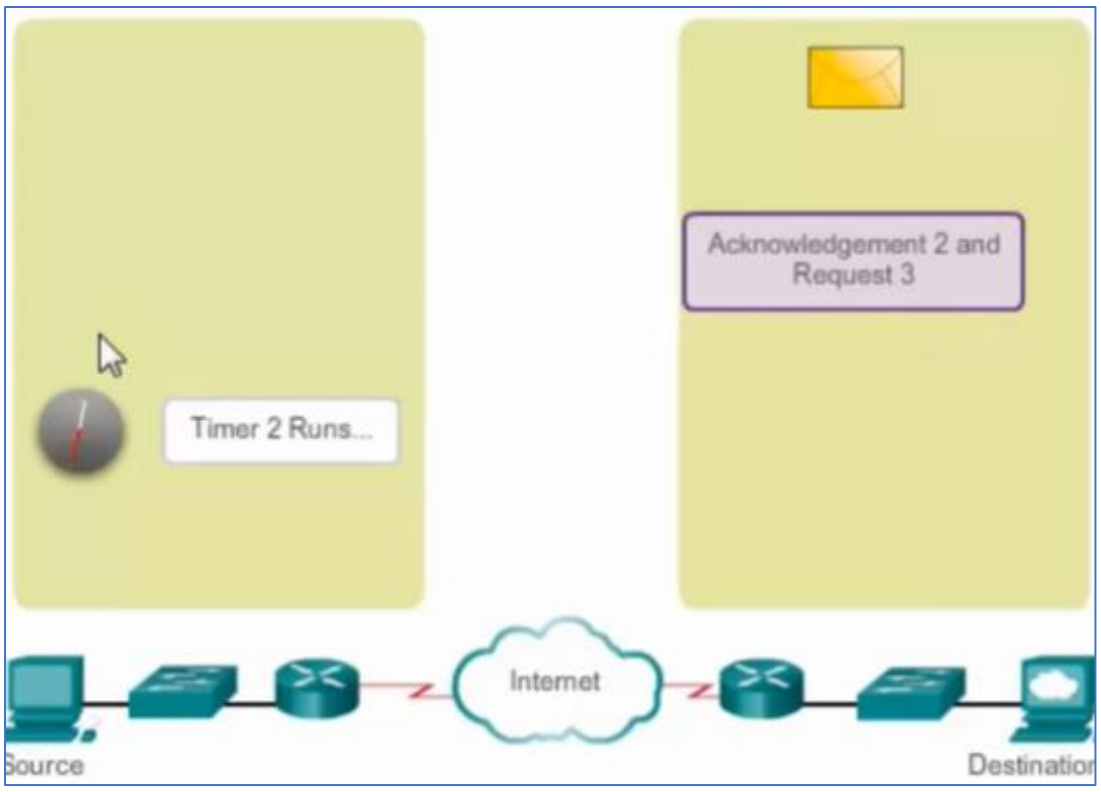
TCP utiliza temporizadores para saber cuánto tiempo debe esperar antes de reenviar un segmento.



9.6.4 Vídeo - Confiabilidad TCP - Pérdida de Datos y Retransmisión

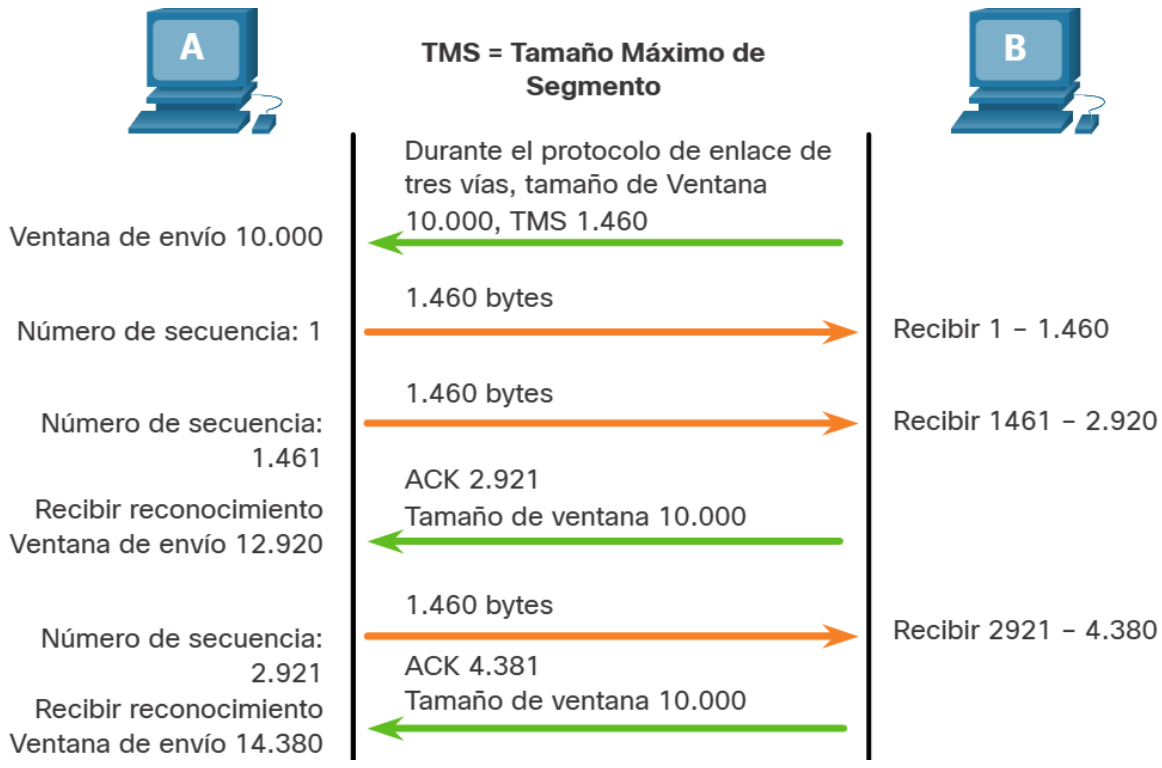
El gráfico que se muestra en este video usa ***números de segmento*** en lugar de ***números de secuencia***. TCP es un protocolo fiable, utiliza números de secuencia y reconocimientos (ACKs) para brindar esa confiabilidad. Pero, ¿qué sucede cuando los datos se pierden en tránsito? Como protocolo confiable, debe haber un mecanismo para reenviar los datos perdidos, para que un total de datos, como un archivo o una imagen, o un video, se pueda reconstruir a partir de todos los segmentos. Si miramos esta animación, podemos ver este proceso en acción. Presionaré reproducir. El host de origen envía el segmento uno e inicia un temporizador. Puede ver que el temporizador se está ejecutando. El host de destino recibe el segmento 1, por tanto, enviará un acuse de recibo. Veamos qué sucede. Podemos ver que el host de destino ha recibido el segmento uno, enviará un ACK1 y un Request 2 ¿Por qué? Recibió el segmento 1, entonces envía una solicitud para el segmento 2 y un ACK 2. Entonces veremos que se envía. Muy bien, ahí va el reconocimiento. El origen recibe el reconocimiento antes de que expire el temporizador y ahora puede enviar el segmento 2. Lo envió y, como puede ver, el temporizador se inició. Esperará para obtener un reconocimiento. Si no recibe un reconocimiento del destino antes de que expire el temporizador, reenviará el segmento 2. Veamos esto en acción. Puede ver que el destino no ha recibido el segmento 2. Como no ha recibido el segmento 2, no enviará un ACK 3 de vuelta a el dispositivo. No reconocerá que recibió el segmento 2 y no enviará un ACK 3 de regreso al host de origen. Veamos qué sucede, si no hay reconocimiento, el temporizador caduca, puede ver aquí el cronómetro caduca. Entonces, ¿qué hará el host de origen? El host de origen retransmitirá o reenviará el segmento 2 y reiniciará el temporizador. Esta vez el destino recibió la información y ahora enviará un ACK 3 solicitando el siguiente dato, en este caso sería el segmento 3. Las confirmaciones recibidas antes de que expire el temporizador y se envía el segmento tres. Se recibe el segmento 3, se envía el ACK 3 y se envía una solicitud de segmento 4 en una confirmación. El reconocimiento se recibe antes de que expire el temporizador y ahora el dispositivo puede enviar el segmento 4, o en este caso es el final de la transmisión. La capacidad de TCP para retransmitir segmentos faltantes hace que las aplicaciones que usan el protocolo TCP sean muy confiables.





9.6.5 Control de Flujo TCP - Tamaño de la Ventana y Acuses de Recibo

TCP también proporciona mecanismos para el control de flujo. El ***control de flujo*** es la cantidad de datos que el destino puede recibir y procesar de manera confiable. El control de flujo permite mantener la confiabilidad de la transmisión de TCP mediante el ajuste de la velocidad del flujo de datos entre el origen y el destino para una sesión dada. Para lograr esto, el encabezado TCP incluye un campo de 16 bits llamado "***tamaño de ventana***". En la figura, se muestra un ejemplo de tamaño de ventana y reconocimientos.



El tamaño de la ventana determina la cantidad de bytes que se pueden enviar para recibir un reconocimiento. El número de reconocimiento es el número del siguiente byte esperado.

El tamaño de ventana es la cantidad de bytes que el dispositivo de destino de una sesión TCP puede aceptar y procesar al mismo tiempo. En este ejemplo, el tamaño de la ventana inicial de la PC B para la sesión TCP es de 10,000 bytes. A partir del primer byte, el byte1, el último byte que la PC A puede enviar sin recibir un reconocimiento es el byte 10000. Esto se conoce como la ventana de envío de la PC A. El tamaño de la ventana se incluye en cada segmento TCP para que el destino pueda modificar el tamaño de la ventana en cualquier momento dependiendo de la disponibilidad del búfer.

El tamaño inicial de la ventana se acuerda cuando se establece la sesión TCP durante la realización del enlace de tres vías. El dispositivo de origen debe limitar el número de bytes enviados al dispositivo de destino en función del tamaño de la ventana del destino. El dispositivo de origen puede continuar enviando más datos para la sesión solo cuando obtiene un reconocimiento de los bytes recibidos. Por lo general, el destino no esperará que se reciban todos los bytes de su tamaño de ventana antes de contestar con un acuse de recibo. A medida que se reciben y procesan los bytes, el destino envía reconocimientos para informar al origen que puede continuar enviando bytes adicionales.

Por ejemplo, es típico que la PC B no espere hasta que se hayan recibido los 10,000 bytes antes de enviar un acuse de recibo. Esto significa que la PC A puede ajustar su ventana de envío a medida que recibe confirmaciones de la PC B. Como se muestra en la figura, cuando la PC A recibe una confirmación con el número de confirmación 2,921, que es el siguiente byte esperado. La ventana de envío de PC A incrementará 2.920 bytes. Esto cambia la ventana de envío de 10.000 bytes a 12.920. Esto significa que la PC A puede ajustar su ventana de envío a medida que recibe confirmaciones de la PC B. Como se muestra en la figura, cuando la PC A recibe una confirmación con el número de confirmación 2,921, que es el siguiente byte esperado.

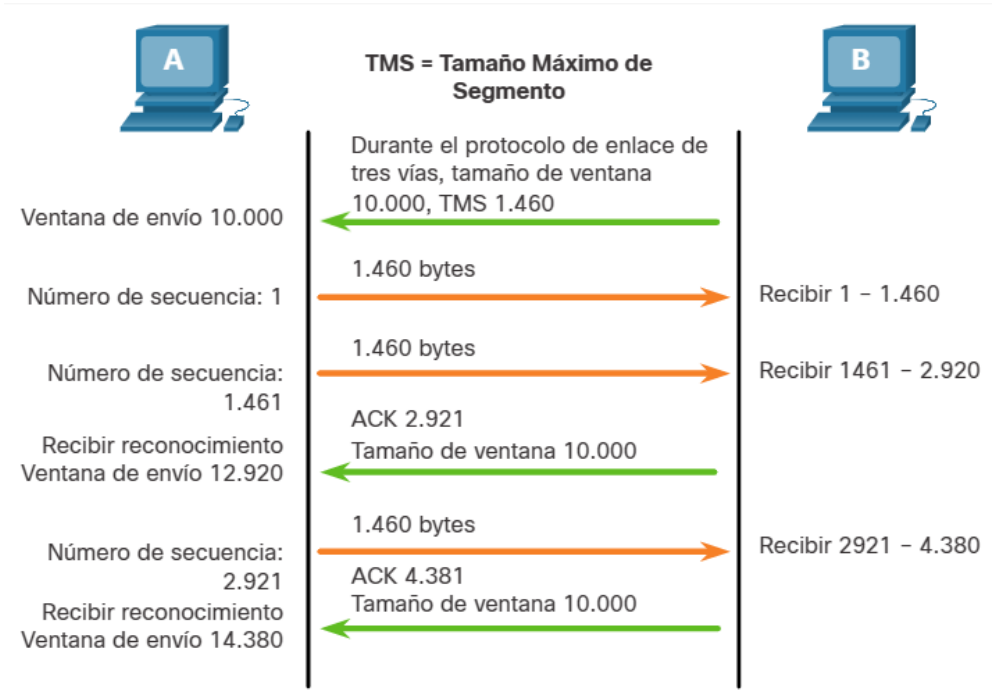
Un destino que envía confirmaciones a medida que procesa los bytes recibidos, y el ajuste continuo de la ventana de envío de origen, se conoce como ***ventanas deslizantes***. En el ejemplo anterior, la ventana de envío del PC A aumenta o se desliza sobre otros 2.921 bytes de 10.000 a 12.920.

Si disminuye la disponibilidad de espacio de búfer del destino, puede reducir su tamaño de ventana para informar al origen que reduzca el número de bytes que debe enviar sin recibir un reconocimiento.

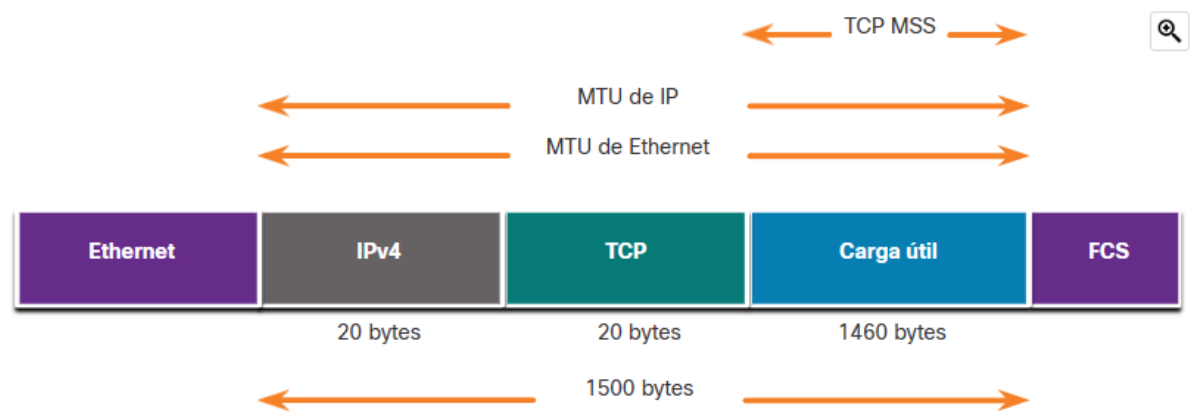
Nota: Hoy en día, los dispositivos utilizan el protocolo de ventanas deslizantes. El receptor generalmente envía un acuse de recibo después de cada dos segmentos que recibe. El número de segmentos recibidos antes de que se acuse recibo puede variar. La ventaja de las ventanas deslizantes es que permiten que el emisor transmita continuamente segmentos mientras el receptor está acusando recibo de los segmentos anteriores. Los detalles de las ventanas deslizantes exceden el ámbito de este curso.

9.6.6 Control de Flujo TCP - Tamaño Máximo de Segmento (MSS)

En la figura, la fuente está transmitiendo 1.460 bytes de datos dentro de cada segmento TCP. Normalmente, es el ***Tamaño Máximo de Segmento*** (**MSS**) que puede recibir el dispositivo de destino. El MSS forma parte del campo de opciones del encabezado TCP que especifica la mayor cantidad de datos, en bytes, que un dispositivo puede recibir en un único segmento TCP. El tamaño MSS no incluye el encabezado TCP. El MSS se incluye normalmente durante el apretón de manos de tres vías.



Un MSS común es de 1.460 bytes cuando se usa IPv4. Un host determina el valor de su campo de MSS restando los encabezados IP y TCP de ***Unidad Máxima de transmisión (MTU)*** de Ethernet. En una interfaz de Ethernet, la MTU predeterminada es de 1500 bytes. Restando el encabezado IPv4 de 20 bytes y el encabezado TCP de 20 bytes, el tamaño predeterminado de MSS será 1460 bytes, como se muestra en la figura.



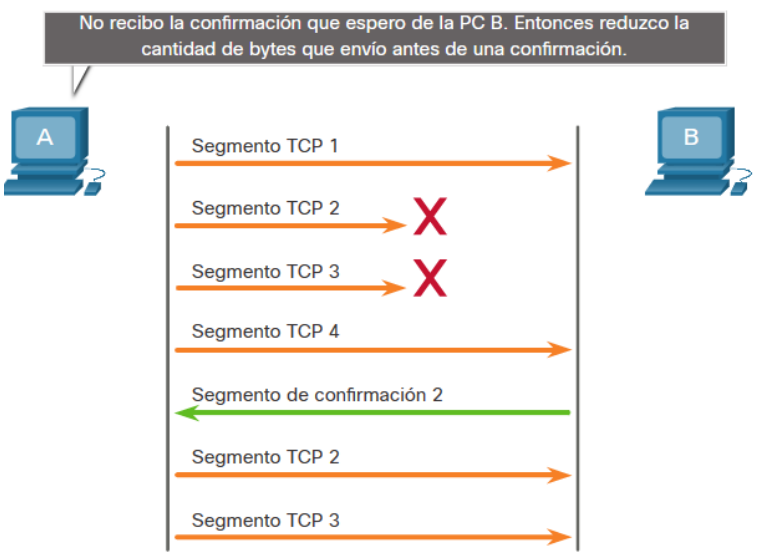
9.6.7 Control de Flujo TCP - Prevención de Congestión

Cuando se produce congestión en una red, el router sobrecargado comienza a descartar paquetes. Cuando los paquetes que contienen segmentos TCP no llegan a su destino, se dejan sin confirmar. Mediante la determinación de la tasa a la que se envían, pero no se reconocen los segmentos TCP, el origen puede asumir un cierto nivel de congestión de la red.

Siempre que haya congestión, se producirá la retransmisión de los segmentos TCP perdidos del origen. Si la retransmisión no se controla adecuadamente, la retransmisión adicional de los segmentos TCP puede empeorar aún más la congestión. No sólo se introducen en la red los nuevos paquetes con segmentos TCP, sino que el efecto de retroalimentación de los segmentos TCP retransmitidos que se perdieron también se sumará a la congestión. Para evitar y controlar la congestión, TCP emplea varios mecanismos, temporizadores y algoritmos de manejo de la congestión.

Si el origen determina que los segmentos TCP no están siendo reconocidos, o reconocidos pero no de una manera oportuna, entonces puede reducir el número de bytes que envía antes de recibir un reconocimiento. Como se ilustra en la figura, PC A detecta que hay congestión y, por lo tanto, reduce el número de bytes que envía antes de recibir un acuse de recibo de PC B.

Control de Congestión de TCP



Los números de acuse de recibo corresponden al siguiente byte esperado y no a un segmento. Los números de segmentos utilizados se simplifican con fines ilustrativos. Tenga en cuenta que es el origen el que está reduciendo el número de bytes sin reconocimiento que envía y no el tamaño de ventana determinado por el destino. **Nota:** La explicación de los mecanismos, temporizadores y algoritmos reales de manejo de la congestión se encuentra fuera del alcance de este curso.

9.6.8 Verifique su Comprensión - Confiabilidad y Control de Flujo

¿Qué campo utiliza el host de destino para volver a ensamblar segmentos en el orden original?

Bits de Control	Puerto de Destino	Numero de secuencia ☺←	Puerto de Origen	Tamaño de la Ventana

¿Qué campo se utiliza para proporcionar control de flujo?

Bits de Control	Puerto de Destino	Numero de secuencia	Puerto de Origen	Tamaño de Ventana ☺←

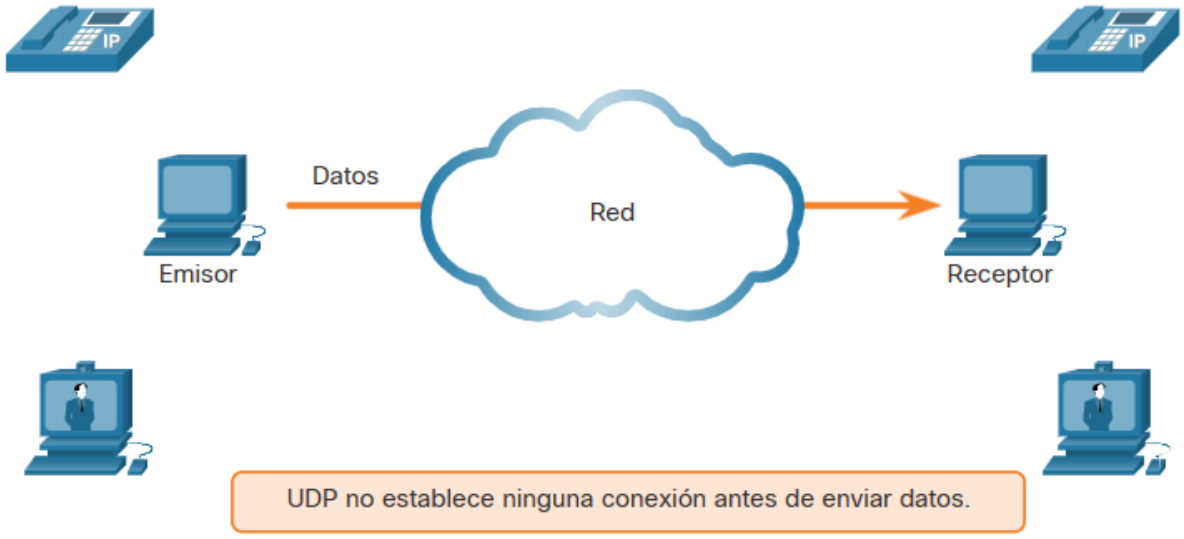
¿Qué sucede cuando un host de envío detecta que hay congestión?

- El host receptor aumenta el número de bytes que envía antes de recibir una confirmación del host remitente.
- El host receptor reduce el número de bytes que envía antes de recibir una confirmación del host remitente.
- El host de envío aumenta el número de bytes que envía antes de recibir una confirmación del host de destino.
- El host de envío reduce el número de bytes que envía antes de recibir una confirmación del host de destino. ☺←

7. Comunicación UDP

9.7.1 Bajo Costo UDP versus Confiabilidad

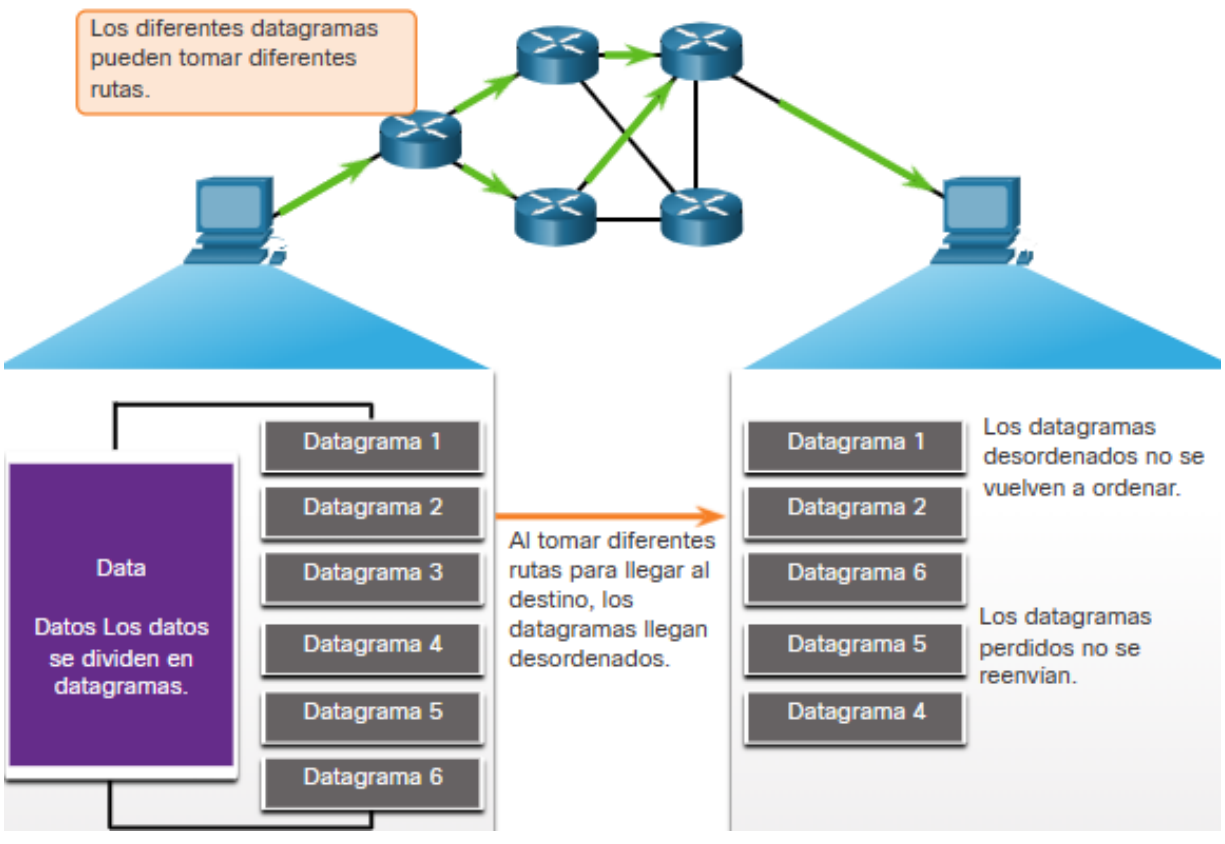
Como se explicó anteriormente, UDP es perfecto para comunicaciones que necesitan ser rápidas, como VoIP. Este tema explica en detalle por qué UDP es perfecto para algunos tipos de transmisiones. Como se muestra en la figura, UDP no establece una conexión. UDP suministra transporte de datos con baja sobrecarga debido a que posee un encabezado de datagrama pequeño sin tráfico de administración de red.



9.7.2 Rearmado de Datagramas UDP

Tal como los segmentos con TCP, cuando se envían datagramas UDP a un destino, a menudo toman diferentes rutas y llegan en el orden equivocado. UDP no realiza un seguimiento de los números de secuencia de la manera en que lo hace TCP. UDP no tiene forma de reordenar datagramas en el orden en que se transmiten, como se muestra en la ilustración. UDP simplemente reensambla los datos en el orden en que se recibieron y los envía a la aplicación. Si la secuencia de datos es importante para la aplicación, esta debe identificar la secuencia adecuada y determinar cómo se deben procesar los datos.

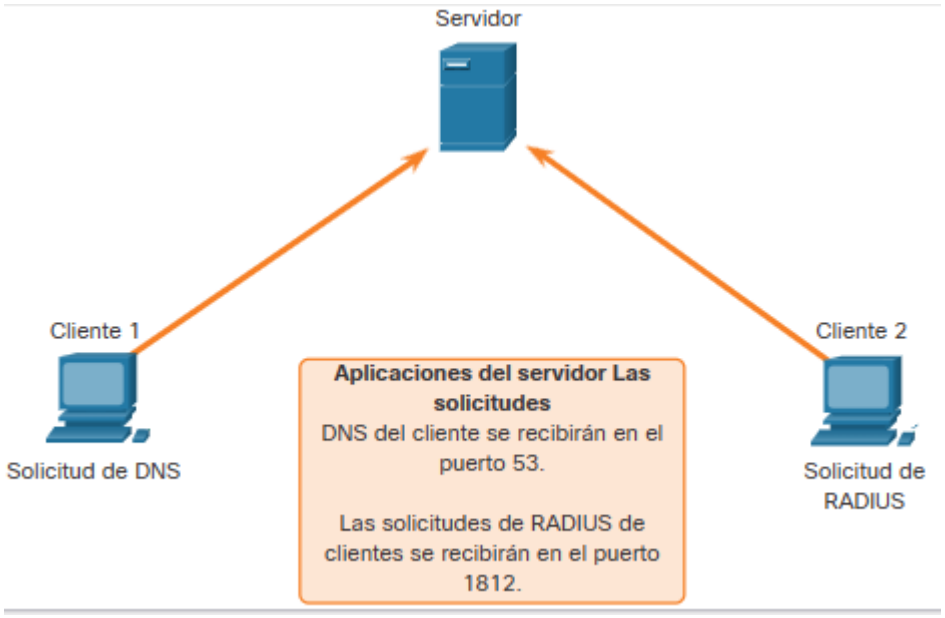
UDP: sin conexión y poco confiable



9.7.3 Procesos y Solicitudes del Servidor UDP

Al igual que las aplicaciones basadas en TCP, a las aplicaciones de servidor basadas en UDP se les asignan números de puerto conocidos o registrados, como se muestra en la figura. Cuando estas aplicaciones o estos procesos se ejecutan en un servidor, aceptan los datos que coinciden con el número de puerto asignado. Cuando UDP recibe un datagrama destinado a uno de esos puertos, envía los datos de aplicación a la aplicación adecuada en base a su número de puerto.

Servidor UDP a la escucha de solicitudes



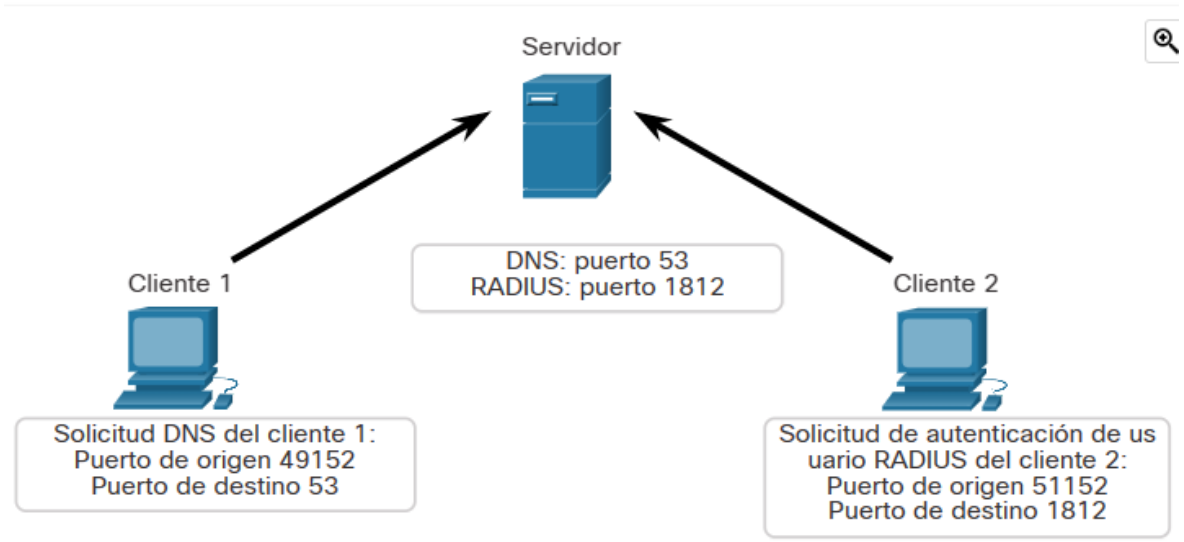
9.7.4 Procesos de Cliente UDP

Como en TCP, la comunicación cliente-servidor es iniciada por una aplicación cliente que solicita datos de un proceso de servidor. El proceso de cliente UDP selecciona dinámicamente un número de puerto del intervalo de números de puerto y lo utiliza como puerto de origen para la conversación. Por lo general, el puerto de destino es el número de puerto bien conocido o registrado que se asigna al proceso de servidor.

Una vez que el cliente selecciona los puertos de origen y de destino, este mismo par de puertos se utiliza en el encabezado de todos los datagramas que se utilizan en la transacción. Para la devolución de datos del servidor al cliente, se invierten los números de puerto de origen y destino en el encabezado del datagrama.

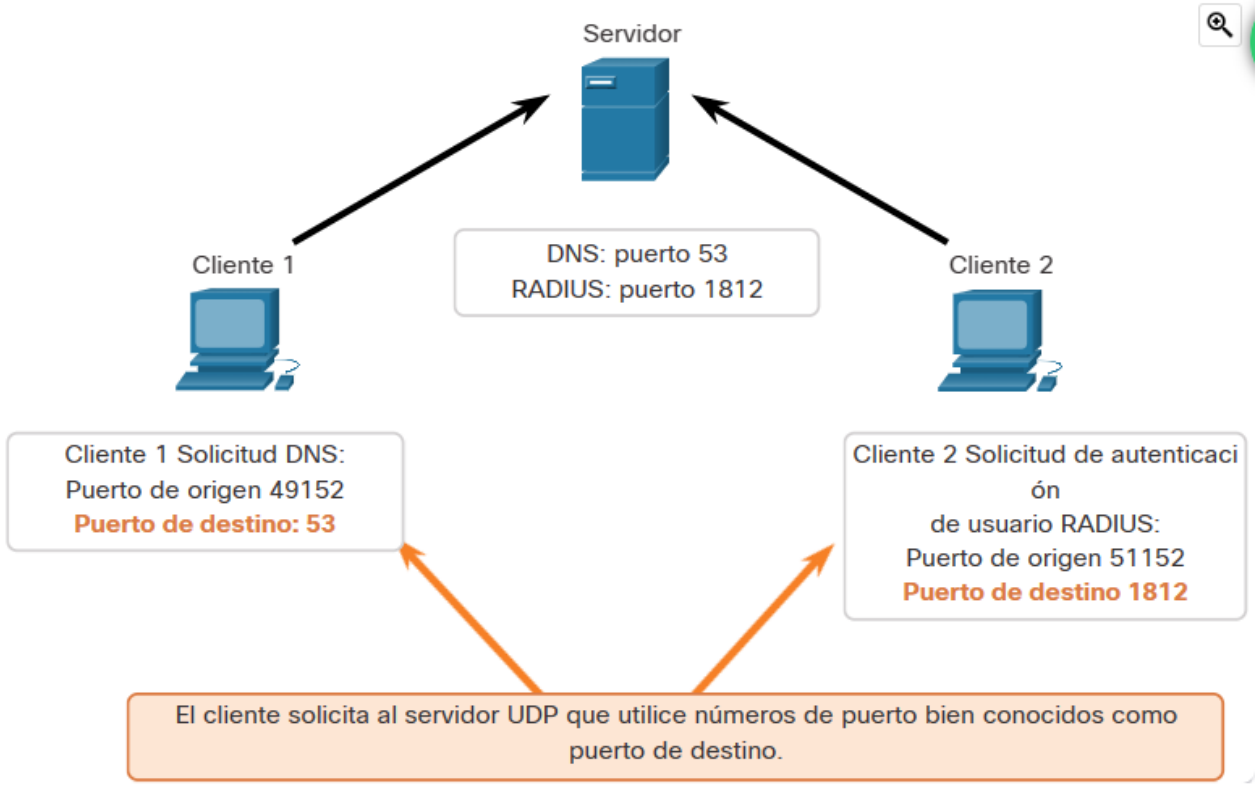
Clientes Enviando Solicitudes UDP

El Cliente 1 envía una solicitud de DNS mientras que el Cliente 2 solicita los servicios de autenticación RADIUS del mismo servidor.



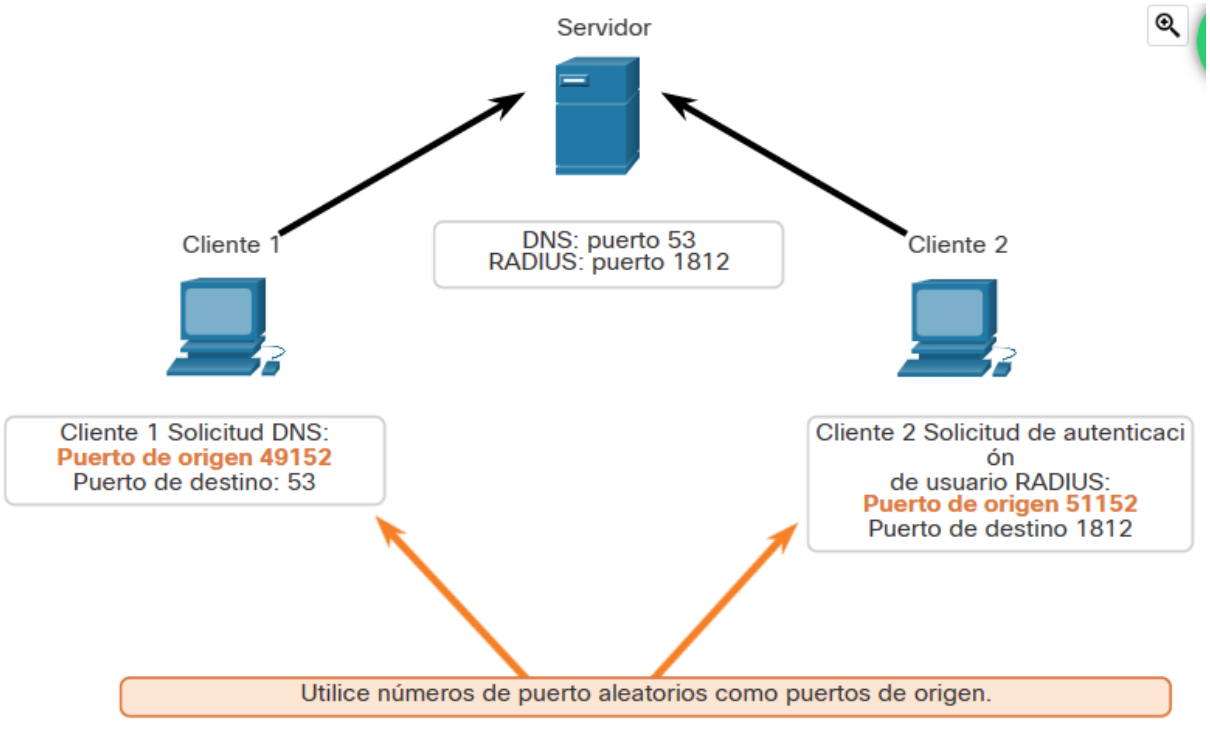
Puertos de Destino de la Solicitud UDP

El cliente 1 está enviando una solicitud DNS utilizando el conocido ***puerto de destino*** 53, mientras que el cliente 2 solicita servicios de autenticación RADIUS mediante el ***puerto registrado*** de destino 1812.



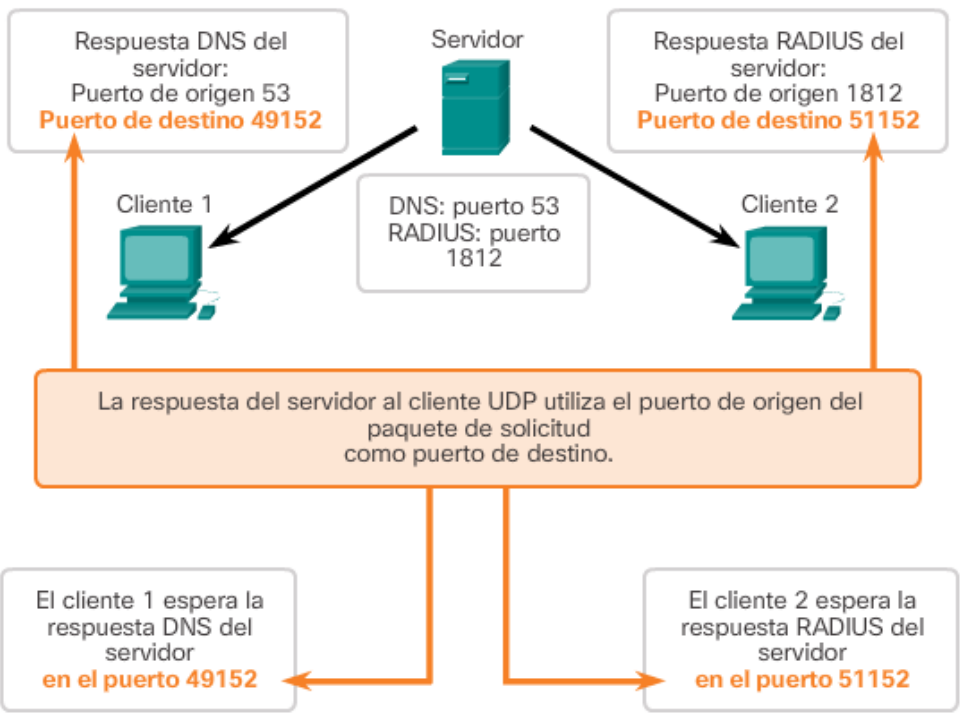
Puertos de Origen de la Solicitud UDP

Las solicitudes de los clientes generan dinámicamente números de puerto de origen. En este caso, el cliente 1 está utilizando el puerto de origen 49152 y el cliente 2 está utilizando el puerto de origen 51152.



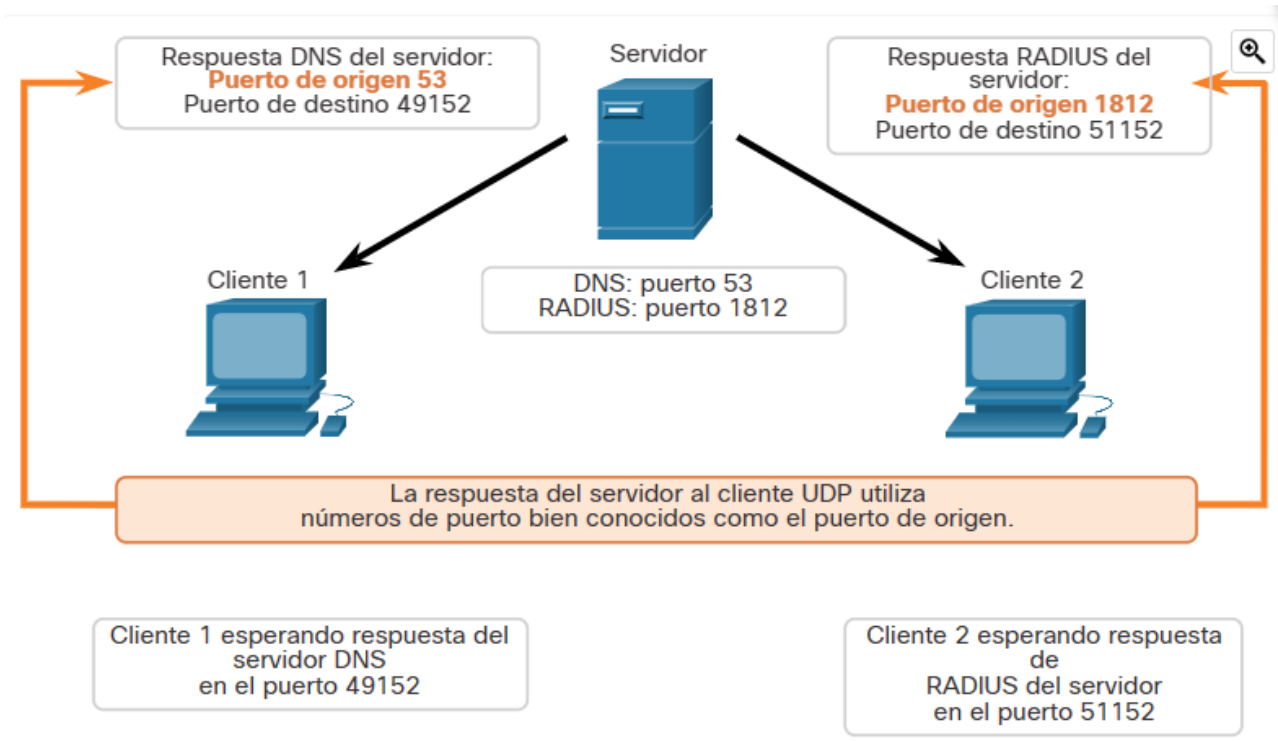
Destino de Respuesta UDP

Cuando el servidor responde a las solicitudes del cliente, invierte los puertos de destino y origen de la solicitud inicial. En la respuesta del servidor a la solicitud DNS ahora el puerto de destino es 49152 y en la respuesta de autenticación RADIUS ahora el puerto de destino es 51152.



Puertos de Origen de Respuesta UDP

Los puertos de origen en la respuesta del servidor son los puertos de destino originales en las solicitudes iniciales.



9.7.5 Verifique su Comprensión - Comunicación UDP

¿Por qué es conveniente UDP para los protocolos que hacen una simple solicitud y responden transacciones?

Control de flujo	Baja sobrecarga ☺←	Confianza	Entrega en el mismo pedido

¿Qué declaración de reensamblaje de datagramas UDP es verdadera?

- UDP no vuelve a ensamblar los datos
- UDP vuelve a ensamblar los datos en el orden en que fueron recibidos. ☺←
- UDP vuelve a ensamblar los datos utilizando bits de control.
- UDP vuelve a ensamblar los datos utilizando números de secuencia.

¿Cuáles de los siguientes puertos serían válidos de origen y destino para un host que se conecta a un servidor DNS?

Fuente: 53, Destino: 49152	Fuente: 1812, Destino: 49152
Fuente: 49152, Destino: 53 ☺←	Fuente: 49152, Destino: 1812

8. Resumen de la Capa de Transporte

9.8.1 Packet Tracer - Comunicaciones TCP y UDP

Packet Tracer: Comunicaciones de TCP y UDP

Objetivos

- Parte 1: Generar tráfico de red en el modo de simulación
- Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

Aspectos básicos

Esta actividad de simulación está destinada a proporcionar una base para comprender TCP y UDP en detalle. El modo de simulación Packet Tracer le proporciona la capacidad de ver el estado de diferentes PDU a medida que viajan a través de la red.

El modo de simulación de Packet Tracer le permite ver cada uno de los protocolos y las PDU asociadas. Los pasos descritos a continuación lo guían a través del proceso de solicitud de servicios de red utilizando diversas aplicaciones que están disponibles en una PC cliente. Explorará la funcionalidad de los protocolos TCP y UDP, la multiplexación y la función de los números de puerto para determinar qué aplicación local solicitó los datos o los envía. Packet Tracer no marcará esta actividad.

Instrucciones

Parte 1: Genere tráfico de red en modo de simulación y vea multiplexación

Paso 1: Generar tráfico para completar las tablas del protocolo de resolución de direcciones (ARP)

Realice la siguiente tarea para reducir la cantidad de tráfico de red que se ve en la simulación.

a. Haga clic en **MultiServer** y luego haga click en **Desktop** tab > **Command Prompt**.

b. Ingrese el comando **ping -n 192.168.1.255**. Está haciendo ping a la dirección de difusión de la LAN del cliente. La opción de comando enviará sólo una solicitud de ping en lugar de las cuatro habituales. Esto tomará unos segundos ya que cada dispositivo en la red responde a la solicitud de ping de MultiServer.

c. Cierre la ventana **MultiServer**.

Paso 2: Generar tráfico web (HTTP).

a. Cambie a modo de simulación.

b. Haga clic en **Cliente HTTP** y abra el **Explorador Web** desde el escritorio.

c. En el campo URL, introduzca **192.168.1.254** y haga clic en **Go** (Ir). Los sobres (PDU) aparecerán en la ventana de topología.

d. Minimice, pero no cierre, la ventana de configuración de **HTTP Client**.

Paso 3: Generar tráfico FTP.

a. Haga clic en **FTP Client** y abra el **Símbolo del Sistema** desde el escritorio

b. Introduzca el comando **ftp 192.168.1.254**. Las PDU aparecerán en la ventana de simulación.

c. Minimice, pero no cierre, la ventana de configuración de **FTP Client**.

Paso 4: Generar tráfico DNS.

a. Haga clic en DNS Client y abra el **Command Prompt**.

b. Introduzca el comando **nslookup multiserver.pt.ptu**. Aparecerá una PDU en la ventana de simulación.

c. Minimice, pero no cierre, la ventana de configuración de **DNS Client**.

Paso 5: Generar tráfico de correo electrónico.

a. Haga clic en **E-Mail Client** y abra la herramienta **E Mail** desde el escritorio.

b. Haga clic en **Compose** (Redactar) y escriba la siguiente información:

1) **To:** user@multiserver.pt.ptu

2) **Subject:** Personalizar la línea de asunto

3) **E-Mail Body:** personalizar el correo electrónico

c. Haga clic en **Send** (Enviar).

d. Minimice, pero no cierre, la ventana de configuración de **E-Mail Client**.

Paso 6: Verificar que se haya generado tráfico y que esté preparado para la simulación. Ahora debería haber entradas de PDU en el panel de simulación para cada uno de los equipos cliente.

Paso 7: Examinar la Multiplexión a medida que el tráfico cruza la red. Ahora utilizará el **botón Capturar/Reenviar (Capture/Forward)** del Panel de Simulación para observar los diferentes protocolos que viajan por la red.

Nota: El botón Capture/Forward ' **>|** ' es una flecha pequeña que apunta a la derecha con una barra vertical al lado.

a. Haga clic una vez en **Capture/Forward**. Todas las PDU se transfieren al switch.

b. Haga clic en **Capturar/Reenviar** seis veces y observe las PDU de los diferentes hosts mientras viajan por la red. Observe que solo una PDU puede cruzar un cable en cada dirección en un momento determinado.

¿Cómo se llama esto? **Conversación multiplexación**.

Aparece una variedad de PDU en la lista de eventos en el Panel de simulación. ¿Cuál es el significado de los diferentes colores? **Representan diferentes protocolos.**

Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

Paso 1: Examinar el tráfico HTTP cuando los clientes se comunican con el servidor.

a. Haga clic en **Reset Simulation (Restablecer simulación)**.

b. Filtrar el tráfico que se muestra actualmente sólo a las PDU **HTTP** y **TCP**. Para filtrar el tráfico que se muestra actualmente:

1) Haga clic en **Edit Filters** y alternar el botón **Show All/None**.

2) Seleccione **HTTP y TCP**. Haga clic en la «x» roja en la esquina superior derecha del cuadro Editar filtros para cerrarla. Los eventos visibles ahora deberían mostrar solo las PDU **HTTP** y **TCP**.

c. Abra el navegador en HTTP Client e ingrese **192.168.1.254** en el campo URL. Haga clic en **Ir** para conectarse al servidor a través de HTTP. Minimice la ventana del Cliente HTTP.

d. Haga clic en **Capturar/Reenviar (Capture/Forward)** hasta que aparezca una PDU para HTTP. Tenga en cuenta que el color del envolvente de la ventana de topología coincide con el código de color de la PDU HTTP del Panel de simulación.

¿Por qué tardó tanto en aparecer la PDU HTTP? Porque TCP primero debe establecer la conexión para que el tráfico HTTP pueda comenzar.

e. Haga clic en el sobre de la PDU para mostrar los detalles de la PDU. Haga clic en **Outbound PDU Details** y desplácese hacia abajo hasta la segunda sección. ¿Cómo se rotula la sección? **TCP**

¿Se consideran confiables estas comunicaciones? **Sí, TCP está en uso.**

Registre los valores de **SRC PORT** (PUERTO DE ORIGEN), **DEST PORT** (PUERTO DE DESTINO), **SEQUENCE NUM** (NÚMERO DE SECUENCIA) y **ACK NUM** (NÚMERO DE RECONOCIMIENTO). **1029 (el valor puede variar), 80, 1, 1**

f. Mire el valor en el campo Indicadores, que se encuentra junto al campo Ventana. Los valores a la derecha de la «b» representan los indicadores TCP que se establecen para esta etapa de la conversación de datos. Cada uno de los seis lugares corresponde a una bandera. La presencia de un «1» en cualquier lugar indica que el indicador está establecido. Se puede configurar más de una bandera a la vez. Los valores de las banderas se muestran a continuación.

Lugar de la bandera	6	5	4	3	2	1
Valor	URG	ACK	PSH	RST	SYN	FIN

¿Qué indicadores TCP se establecen en esta PDU? **ACK y PSH**

g. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU con una marca de verificación regrese al **HTTP Client**.

h. Cierre el sobre de PDU y seleccione **Inbound PDU Details**.

¿En qué cambiaron los números de puerto y de secuencia? **Los puertos de origen y destino están invertidos, y el número de reconocimiento es 1. Las banderas han cambiado a SYN + ACK.**

i. Haga clic en la PDU **HTTP que HTTP Client** ha preparado para enviar a **MultiServer.** Este es el comienzo de la comunicación HTTP. Haga clic en este segundo sobre de PDU y seleccione **Outbound PDU Details** (Detalles de PDU saliente). ¿Qué información aparece ahora en la sección TCP? ¿En qué se diferencian los números de puerto y de secuencia con respecto a las dos PDU anteriores? **Los puertos de origen y destino se invierten, el número de secuencia es 1, el número de reconocimiento es 103 (el valor puede variar) y los indicadores son PSH y ACK.**

Paso 2: Examinar el tráfico FTP cuando los clientes se comunican con el servidor.

a. Abra el símbolo del sistema en el escritorio del cliente FTP. Inicie una conexión FTP ingresando **ftp 192.168.1.254**.

b. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **FTP** y **TCP**.

c. Haga clic en **Capture/Forward**. Haga clic en el segundo sobre PDU para abrirlo.

Haga clic en la pestaña **Outbound PDU Details** y desplácese hacia abajo hasta la sección TCP.

¿Se consideran confiables estas comunicaciones? **Si.**

d. Registre los valores de **SRC PORT** (PUERTO DE ORIGEN), **DEST PORT** (PUERTO DE DESTINO), **SEQUENCE NUM** (NÚMERO DE SECUENCIA) y **ACK NUM** (NÚMERO DE RECONOCIMIENTO). ¿Cuál es el valor en el campo de bandera? **1025, 21, 0, 0. SYN**

e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **FTP Client** con una marca de verificación.

f. Cierre el sobre de PDU y seleccione **Inbound PDU Details**.

¿En qué cambiaron los números de puerto y de secuencia? **21, 1025, 0, 1. SYN+ACK. Los puertos de origen y destino están invertidos, y el número de reconocimiento es 1.**

g. Haga clic en la pestaña **Outbound PDU Details**. ¿En qué se diferencian los números de puerto y secuencia de los resultados anteriores? **1025, 21, 1, 1. Los puertos de origen y destino están invertidos, y tanto el número de secuencia como el de reconocimiento son 1.**

h. Cierre la PDU y haga clic en **Capture/Forward** hasta que una segunda PDU vuelva a **FTP Client**. La PDU es de un color diferente.

i. Abra la PDU y seleccione **Inbound PDU Details**. Desplácese hasta después de la sección TCP.

¿Cuál es el mensaje del servidor? **«Bienvenido al servidor FTP PT»**

j. Haga clic en Reset Simulation (Restablecer simulación).

Paso 3: Examinar el tráfico DNS cuando los clientes se comunican con el servidor.

a. Repita los pasos de la Parte 1 para crear tráfico DNS.

b. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **DNS** y **UDP**.

c. Haga clic en el sobre de PDU para abrirlo.

d. Mire los detalles del modelo OSI para la PDU saliente.

¿Qué es el protocolo de capa 4? **UDP.**

¿Se consideran confiables estas comunicaciones? **No.**

e. Abra la ficha Detalles de PDU saliente y busque la sección UDP de los formatos de PDU. Registre los valores de **SRC PORT** (PUERTO DE ORIGEN) y **DEST PORT** (PUERTO DE DESTINO). ¿Por qué no hay números de secuencia y reconocimiento? **1025 (el valor puede variar) y 53.**

f. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU con una marca de verificación regrese al **DNS Client**.

g. Cierre el sobre de PDU y seleccione **Inbound PDU Details**.

¿En qué cambiaron los números de puerto y de secuencia? **53, 1025. Los puertos de origen y destino están invertidos.**

¿Cómo se llama la última sección de la **PDU**? ¿Cuál es la dirección IP para el nombre **multiserver.pt.ptu**? **RESPUESTA DNS, 192.1681.254.**

h. Haga clic en Reset Simulation (Restablecer simulación).

Paso 4: Examinar el tráfico de correo electrónico cuando los clientes se comunican con el servidor.

a. Repita los pasos de la Parte 1 para enviar un correo electrónico a **user@multiserver.pt.ptu**.

b. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **POP3, SMTP** y **TCP**.

c. Haga clic en el primer sobre de la PDU para abrirlo.

d. Haga clic en la pestaña **Outbound PDU Details** y desplácese hacia abajo hasta la última sección.

¿Qué protocolo de la capa de transporte utiliza el tráfico de correo electrónico? **TCP.**

¿Se consideran confiables estas comunicaciones? **Si.**

e. Registre los valores de **SRC PORT** (PUERTO DE ORIGEN), **DEST PORT** (PUERTO DE DESTINO), **SEQUENCE NUM** (NÚMERO DE SECUENCIA) y **ACK NUM** (NÚMERO DE RECONOCIMIENTO). ¿Cuál es el valor del campo de bandera?

1025 (el valor puede variar), 25, 0, 0. SYN

f. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU regrese al **E-Mail Client** con una marca de verificación.

g. Haga clic en el sobre TCP PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

25, 1025, 0, 1. SYN+ACK. Los puertos de origen y destino están invertidos, y el número de reconocimiento es 1.

h. Haga clic en la pestaña **Outbound PDU Details**. ¿En qué se diferencian los números de puerto y de secuencia con respecto a los dos resultados anteriores? **1025, 25, 1, 1. ACK. Los puertos de origen y destino están invertidos, y tanto el número de secuencia como el de reconocimiento son 1. ACK**

i. Hay una segunda **PDU** de un color diferente que **E-Mail Client** ha preparado para enviar a **MultiServer**. Este es el comienzo de la comunicación de correo electrónico. Haga clic en este segundo sobre de PDU y seleccione **Outbound PDU Details**.

¿En qué se diferencian los números de puerto y de secuencia con respecto a las dos PDU anteriores? **1025, 25, 1, 1. PSH+ACK. Los puertos de origen y destino están invertidos, y tanto el número de secuencia como el de reconocimiento son 1.**

¿Qué protocolo de correo electrónico se relaciona con el puerto TCP 25? ¿Qué protocolo se relaciona con el puerto TCP 110? **SMTP. POP3.**

9.8.2 ¿Qué Aprendí en este Módulo?

LA CAPA TRANSPORTE

Los programas de la capa Aplicación generan datos que deben intercambiarse entre los hosts de origen y de destino. La capa Transporte es responsable de las comunicaciones lógicas entre aplicaciones que se ejecutan en diferentes hosts e incluye dos protocolos: Protocolo de control de transmisión TCP y Protocolo de datagramas de usuario UDP.

- Seguimiento de conversaciones individuales - En la capa Transporte, cada conjunto de datos que fluye entre una aplicación de origen y una aplicación de destino se conoce como conversación y se realiza un seguimiento por separado. Es responsabilidad de la capa Transporte mantener y hacer un seguimiento de todas estas conversaciones.
- Segmentación de Datos y Reensamblaje de Segmentos - Es responsabilidad de la capa Transporte dividir los datos de la aplicación en bloques de tamaño adecuado. Dependiendo del protocolo utilizado, los bloques de la capa Transporte se denominan segmentos o datagramas.
- Agregar Información del Encabezado - El protocolo de la capa Transporte también agrega información de encabezado que contiene datos binarios organizados en varios campos para cada bloque de datos.
- Identificación de las Aplicaciones - La capa Transporte debe poder separar y administrar múltiples comunicaciones con diferentes necesidades de requisitos de transporte.
- Multiplexación de Conversaciones - El envío de algunos tipos de datos (por ejemplo, una transmisión de video) a través de una red, como una transmisión de comunicación completa, puede consumir todo el ancho de banda disponible. La capa Transporte utiliza segmentación y multiplexación para permitir que diferentes conversaciones de comunicación se intercalen en la misma red.

Los protocolos TCP/UDP de la capa Transporte especifican cómo transferir mensajes entre hosts y son responsables de administrar los requisitos de fiabilidad de una conversación.

TCP proporciona confiabilidad y control de flujo mediante estas operaciones básicas:

- Numerar y rastrear segmentos de datos transmitidos a un host específico desde una aplicación específica
- Reconocer los datos recibidos
- Volver a transmitir cualquier información no reconocida después de un cierto período de tiempo
- Datos de secuencia que pueden llegar en un orden incorrecto
- Enviar datos a una velocidad eficiente que sea aceptable por el receptor

Para mantener el estado de una conversación y realizar un seguimiento de la información, TCP debe establecer primero una conexión entre el remitente y el receptor. Es por eso que TCP se conoce como un ***protocolo orientado a la conexión***.

UDP es un protocolo sin conexión. Debido a que UDP no proporciona fiabilidad ni control de flujo, no requiere una conexión establecida. Debido a que UDP no realiza un seguimiento de la información enviada o recibida entre el cliente y el servidor, UDP también se conoce como ***protocolo sin estado***. UDP también se conoce como un ***protocolo de entrega de mejor esfuerzo*** porque no hay reconocimiento de que los datos se

reciben en el destino. Con UDP, no existen procesos de capa de transporte que informen al emisor si la entrega se realizó correctamente. UDP es preferible para aplicaciones como Voz sobre IP (VoIP). Los reconocimientos y la retransmisión retrasarían la entrega y harían inaceptable la conversación de voz. UDP también es utilizado por las aplicaciones de solicitud y respuesta donde los datos son mínimos, y la retransmisión se puede hacer rápidamente.

Para otras aplicaciones es importante que todos los datos lleguen y que puedan ser procesados en su secuencia adecuada. Para estos tipos de aplicaciones, TCP se utiliza como protocolo de transporte. Por ejemplo, las aplicaciones como las bases de datos, los navegadores web y los clientes de correo electrónico, requieren que todos los datos que se envían lleguen a destino en su formato original. Cualquier dato faltante podría corromper una comunicación, haciéndola incompleta o ilegible.

DESCRIPCION GENERAL DE TCP

Además de admitir las funciones básicas de segmentación y reensamblado de datos, TCP también proporciona los siguientes servicios:

- Establece una sesión - TCP es un protocolo orientado a la conexión que negocia y establece una conexión permanente (o sesión) entre los dispositivos de origen y destino antes de reenviar cualquier tráfico. Mediante el establecimiento de sesión, los dispositivos negocian la cantidad de tráfico que se puede reenviar en un momento determinado, y los datos que se comunican entre ambos se pueden administrar detenidamente.
- Garantiza una entrega confiable - Por muchas razones, es posible que un segmento se corrompa o se pierda por completo, ya que se transmite a través de la red. TCP asegura que cada segmento que envía la fuente llega al destino.
- Proporciona entrega en el mismo orden - Debido a que las redes pueden proporcionar múltiples rutas que pueden tener diferentes velocidades de transmisión, los datos pueden llegar en el orden incorrecto. Al numerar y secuenciar los segmentos, TCP garantiza que los segmentos se vuelvan a ensamblar en el orden correcto.
- Admite control de flujo - Los hosts de red tienen recursos limitados (es decir, memoria y potencia de procesamiento). Cuando TCP advierte que estos recursos están sobrecargados, puede solicitar que la aplicación emisora reduzca la velocidad del flujo de datos. Esto lo lleva a cabo TCP, que regula la cantidad de datos que transmite el origen. El control de flujo puede evitar la necesidad de retransmitir los datos cuando los recursos del host receptor se ven desbordados.

TCP es un protocolo con estado, lo que significa que realiza un seguimiento del estado de la sesión de comunicación. Para hacer un seguimiento del estado de una sesión, TCP registra qué información se envió y qué información se reconoció. La sesión con estado comienza con el establecimiento de la sesión y termina con la finalización de la sesión.

Los diez campos en el encabezado TCP son los siguientes:

- Puerto de Origen - Un campo de 16 bits que se utiliza para identificar la aplicación de origen por número de puerto.
- Puerto de Destino - Un campo de 16 bits que se utiliza para identificar la aplicación de destino por número de puerto.
- Número de Secuencia - Un campo de 32 bits que se utiliza para fines de reensamblaje de datos.
- Número de Acuse de Recibo - Un campo de 32 bits que se utiliza para indicar que se han recibido datos y que se espera el próximo byte de la fuente.
- Longitud del Encabezado - Un campo de 4 bits conocido como "desplazamiento de datos" que indica la longitud del encabezado del segmento TCP.
- Reservado - Un campo de 6 bits que está reservado para uso futuro.
- Bits de Control - Un campo de 6 bits que incluye códigos de bits o indicadores que indican el propósito y la función del segmento TCP.
- Tamaño de la Ventana - Un campo de 16 bits que se utiliza para indicar el número de bytes que se pueden aceptar a la vez.
- Suma de Comprobación - Un campo de 16 bits que se utiliza para la comprobación de errores del encabezado y los datos del segmento.
- Urgente - Un campo de 16 bits que se utiliza para indicar si los datos contenidos son urgentes.

TCP es un buen ejemplo de cómo las diferentes capas del conjunto de protocolos TCP/IP tienen roles específicos. TCP maneja todas las tareas asociadas con la división del flujo de datos en segmentos, proporcionando confiabilidad, controlando el flujo de datos y reordenando segmentos. TCP libera la aplicación de tener que administrar estas tareas. HTTP, FTP, SMTP y SSH pueden simplemente enviar el flujo de datos a la capa de transporte y usar los servicios de TCP.

DESCRIPCION GENERAL DE UDP

UDP es un protocolo de transporte liviano que ofrece la misma segmentación y rearmado de datos que TCP, pero sin la confiabilidad y el control del flujo de TCP.

Las características UDP incluyen lo siguiente:

- Los datos se reconstruyen en el orden en que se recibieron.
- Los segmentos perdidos no se vuelven a enviar.
- No hay establecimiento de sesión.
- El envío no está informado sobre la disponibilidad de recursos.

UDP es un protocolo sin estado, lo que significa que ni el cliente ni el servidor rastrean el estado de la sesión de comunicación. Si se requiere confiabilidad al utilizar UDP como protocolo de transporte, a esta la debe administrar la aplicación.

Los bloques de comunicación en UDP se denominan datagramas o segmentos. Estos datagramas se envían como el mejor esfuerzo por el protocolo de la capa de transporte. El encabezado UDP es mucho más simple que el encabezado TCP porque solo tiene cuatro campos y requiere 8 bytes (es decir, 64 bits).

Los cuatro campos en el encabezado UDP son los siguientes:

- Puerto de Origen - Un campo de 16 bits que se utiliza para identificar la aplicación de origen por número de puerto.
- Puerto de Destino - Un campo de 16 bits que se utiliza para identificar la aplicación de destino por número de puerto.
- Longitud - Un campo de 16 bits que indica la longitud del encabezado del datagrama UDP.
- Suma de Comprobación - Un campo de 16 bits que se utiliza para la comprobación de errores del encabezado y los datos del datagrama.

Hay tres tipos de aplicaciones que se adaptan mejor a UDP: aplicaciones de video en vivo y multimedia, aplicaciones simples de solicitud y respuesta, aplicaciones que manejan la confiabilidad por sí mismas.

NÚMEROS DE PUERTO

Los protocolos de capa de transporte TCP y UDP utilizan números de puerto para administrar múltiples conversaciones simultáneas. Los campos de encabezado TCP y UDP identifican un número de puerto de origen y destino de la aplicación. El número de puerto de origen está asociado con la aplicación de origen en el host local, mientras que el número de puerto de destino está asociado con la aplicación de destino en el host remoto.

Los puertos de origen y de destino se colocan dentro del segmento. Los segmentos se encapsulan dentro de un paquete IP. El paquete IP contiene la dirección IP de origen y de destino. Se conoce como ***socket*** a la ***combinación de la dirección IP de origen y el número de puerto de origen***, o de la dirección IP de destino y el número de puerto de destino.

El socket se utiliza para identificar el servidor y el servicio que solicita el cliente. Un socket de cliente puede ser parecido a esto, donde 1099 representa el número de puerto de origen: 192.168.1.5:1099 El socket en un servidor web podría ser el siguiente: 192.168.1.7:80 Juntos, estos dos sockets se combinan para formar un par de sockets: 192.168.1.5:1099, 192.168.1.7:80 Los sockets permiten que los diversos procesos que se ejecutan en un cliente se distingan entre sí. También permiten la diferenciación de diferentes conexiones a un proceso de servidor.

La IANA es la organización de estándares responsable de asignar varios estándares de direccionamiento, incluidos los números de puerto de 16 bits. Los 16 bits utilizados para identificar los números de puerto de origen y destino proporcionan un rango de puertos entre 0 y 65535.

La IANA ha dividido el rango de números en los siguientes tres grupos de puertos:

- Puertos Bien Conocidos (0 a 1,023)
- Puertos Registrados (1,024 a 49,151)
- Puertos Privados y/o Dinámicos (49,152 a 65,535)

Las conexiones TCP no identificadas pueden representar una importante amenaza a la seguridad. Pueden indicar que algo o alguien está conectado al host local. Netstat es una utilidad de red importante que puede usarse para verificar esas conexiones. Ingrese el comando netstat para enumerar los protocolos en uso, la dirección local y los números de puerto, la dirección externa y los números de puerto, y el estado de la conexión. De forma predeterminada, el comando netstat intentará resolver las direcciones IP en nombres de dominio y los números de puerto en aplicaciones conocidas.

PROCESO DE COMUNICACIÓN TCP

La razón por la que TCP es el mejor protocolo para algunas aplicaciones es porque, a diferencia de UDP, reenvía paquetes descartados y paquetes numerados para indicar su orden correcto antes de la entrega. TCP también puede ayudar a mantener el flujo de paquetes para que los dispositivos no se sobrecarguen.

Los números de secuencia se asignan en el encabezado de cada paquete para garantizar que todos los segmentos lleguen en el orden correcto al destino. El número de secuencia representa el primer byte de datos del segmento TCP. Durante la configuración de la sesión, se establece un número de secuencia inicial (ISN). Este ISN representa el valor inicial de los bytes que se transmiten a la aplicación receptora. A medida que se transmiten los datos durante la sesión, el número de secuencia se incrementa según el número de bytes que se han transmitido. Este seguimiento de bytes de datos permite identificar y reconocer cada segmento de manera exclusiva. A partir de esto, se pueden identificar segmentos perdidos.

El número de secuencia (SEQ) y el número de acuse de recibo (ACK) se utilizan juntos para confirmar la recepción de los bytes de datos contenidos en los segmentos transmitidos. El número SEQ identifica el primer byte de datos en el segmento que se transmite. TCP utiliza el número de ACK reenviado al origen para indicar el próximo byte que el receptor espera recibir. Esto se llama acuse de recibo de expectativa.

TCP también proporciona mecanismos para el control de flujo. El control de flujo es la cantidad de datos que el destino puede recibir y procesar de manera confiable. El control de flujo permite mantener la confiabilidad de la transmisión de TCP mediante el ajuste de la velocidad del flujo de datos entre el origen y el destino para una sesión dada. Para lograr esto, el encabezado TCP incluye un campo de 16 bits llamado “tamaño de la ventana”.

El tamaño de la ventana determina la cantidad de bytes que se pueden enviar para recibir un reconocimiento. El número de reconocimiento es el número del siguiente byte esperado. El tamaño inicial de la ventana se acuerda cuando se establece la sesión TCP durante la realización del enlace de tres vías. El dispositivo de origen debe limitar el número de bytes enviados al dispositivo de destino en función del tamaño de la ventana del destino. El dispositivo de origen puede continuar enviando más datos para la sesión solo cuando obtiene un reconocimiento de los bytes recibidos.

El MSS forma parte del campo de opciones del encabezado TCP que especifica la mayor cantidad de datos, en bytes, que un dispositivo puede recibir en un único segmento TCP. El tamaño MSS no incluye el encabezado TCP. El MSS se incluye normalmente durante el apretón de manos de tres vías.

Siempre que haya congestión, se producirá la retransmisión de los segmentos TCP perdidos del origen. Si la retransmisión no se controla adecuadamente, la retransmisión adicional de los segmentos TCP puede empeorar aún más la congestión. Para evitar y controlar la congestión, TCP emplea varios mecanismos, temporizadores y algoritmos de manejo de la congestión.

COMUNICACIONES UDP

UDP no establece ninguna conexión. UDP suministra transporte de datos con baja sobrecarga debido a que posee un encabezado de datagrama pequeño sin tráfico de administración de red.

Tal como los segmentos con TCP, cuando se envían datagramas UDP a un destino, a menudo toman diferentes rutas y llegan en el orden equivocado. UDP no realiza un seguimiento de los números de secuencia de la manera en que lo hace TCP. Por lo tanto, UDP simplemente reensambla los datos en el orden en que se recibieron y los envía a la aplicación.

Al igual que las aplicaciones basadas en TCP, a las aplicaciones de servidor basadas en UDP se les asignan números de puerto bien conocidos o registrados. Cuando estas aplicaciones o estos procesos se ejecutan en un servidor, aceptan los datos que coinciden con el número de puerto asignado. Cuando UDP recibe un datagrama destinado a uno de esos puertos, envía los datos de aplicación a la aplicación adecuada en base a su número de puerto.

Después de que un cliente ha seleccionado los puertos de origen y destino, se utiliza el mismo par de puertos en el encabezado de todos los datagramas en la transacción. Para la devolución de datos del servidor al cliente, se invierten los números de puerto de origen y destino en el encabezado del datagrama.

9.8.3 Webster - Preguntas de Reflexión

Este módulo tenía mucha información sobre la capa de transporte. ¡Nunca supe que sucedió tanto aquí! ¿Lo hizo? Cuando visitaba un sitio web o enviaba un correo electrónico, ¿pensaba en lo diferente que era eso a unirse a una videollamada? ¿Por qué es uno más confiable? ¿Por qué siempre recibe cada palabra en un mensaje de correo electrónico, pero a veces pierde una palabra en su videollamada? Ahora debe tener algún conocimiento sobre la diferencia entre TCP y UDP. ¡Estoy emocionado de tomar este curso y espero que usted también lo haga!

9.8.4 Prueba de La Capa de Transporte

Haga coincidir las características con los protocolos correctos.

CONTROL DE FLUJO	TCP		DEPENDIENTE DE LA CORRECCION DE ERRORES	UDP
CONFIABLE	TCP		NUMERO DE SECUENCIA	TCP
ENTREGA EFICIENTE	TCP		MENOS SOBRECARGA	UDP

¿Qué enunciado describe correctamente la transmisión de datos en la capa de transporte?

- La retransmisión de paquetes perdidos es proporcionada por TCP y UDP.
- La segmentación la proporciona el campo de tamaño de ventana cuando se utiliza el protocolo TCP.
- Un solo datagrama puede incluir un encabezado TCP y UDP.
- Tanto UDP como TCP utilizan números de puerto. ☺←
- La segmentación se proporciona por números de secuencia cuando se utiliza UDP.

¿Cuáles tres campos se utilizan en un encabezado de segmento UDP? (Escoja tres opciones).

Tamaño de la Ventana	Duración ☺←
Puerto de origen ☺←	Número de Acuse de Recibo
Suma de Comprobación ☺←	Número de Secuencia

¿Cuál es el último segmento enviado para completar el proceso de finalización de una sesión TCP iniciada por un cliente?

- un segmento con el indicador ACK establecido en 1 desde el cliente ☺←
- un segmento con el indicador FIN establecido en 1 desde el servidor
- un segmento con el indicador SYN establecido en 1 desde el cliente
- un segmento con el indicador ACK establecido en 1 desde el servidor

¿Cuál de las siguientes es una característica de proceso de servidores TCP?

- Cada proceso de aplicación en ejecución en el servidor se debe configurar para utilizar un número de puerto dinámico.
- Pueden existir muchos puertos abiertos simultáneamente en un servidor, uno para cada aplicación de servidor activa. ☺←
- Un servidor individual puede tener dos servicios asignados al mismo número de puerto dentro de los mismos servicios de la capa de transporte.
- Un host que está ejecutando dos aplicaciones diferentes puede tenerlas configuradas para que utilicen el mismo puerto del servidor.

La congestión de la red hizo que el emisor note la pérdida de segmentos TCP que se enviaron a destino. ¿Cuál de las siguientes es una forma en la que el protocolo TCP intenta solucionar este problema?

- El origen reduce la cantidad de datos que transmite antes de recibir un acuse de recibo del destino. ☺←
- El origen reduce el tamaño de la ventana para reducir la velocidad de transmisión del destino.
- El destino reduce el tamaño de la ventana.
- El destino envía menos cantidad de mensajes de acuse de recibo para conservar el ancho de banda.

¿Qué campo en el encabezado TCP indica el estado del three-way handshake?

Ventana	Reservado	Checksum	Bits de control ☺←

¿Cuáles de las siguientes son dos características de los protocolos que se utilizan dentro de la pila del protocolo TCP/IP? (Escoja dos opciones).

- El protocolo IP de la capa de Internet tiene mecanismos integrados para garantizar la transmisión y la recepción confiables de los datos.
- UDP se utiliza cuando una aplicación se debe entregar lo más rápidamente posible y se puede tolerar alguna pérdida de datos. ☺←
- Los números de los puertos de destino de TCP y UDP son generados dinámicamente por el dispositivo emisor a fin de rastrear las respuestas a las solicitudes.
- Los mecanismos de TCP retransmiten los datos cuando no se recibe un acuse de recibo del sistema de destino dentro de un período establecido ☺←
- El mismo puerto de origen de la capa de transporte se utiliza para todas las pestañas abiertas al mismo tiempo dentro de un navegador web.

Haga coincidir cada descripción con el mecanismo TCP correspondiente.

recibido por un remitente antes de transmitir más segmentos en una sesión	✓ acuse de recibo
número de bytes que un dispositivo de destino puede aceptar y procesar al mismo tiempo	✓ tamaño de ventana
método de gestión de segmentos ante pérdida de datos	✓ retransmisión
se utiliza para identificar segmentos faltantes de datos	✓ números de secuencia

Haga coincidir la descripción con TCP o UDP.

Está orientado a la conexión	
TCP	✓
Sin conexión	
UDP	✓
Usa acuses de recibo	
TCP	✓
Tiene un encabezado grande	
TCP	✓
Es adecuado para aplicaciones intolerantes a demoras	
UDP	✓
Protocolo de entrega de mejor esfuerzo	
UDP	✓

¿Cuál de las siguientes es una característica del protocolo UDP?

Baja sobrecarga ☺←	Entrega garantizada
Corrección de errores	Establecimiento de extremo a extremo antes de la entrega

¿Cuáles dos indicadores en el encabezado de la PDU de capa 4 configuran un cliente y un servidor para finalizar una conversación TCP? (Elija dos opciones).

URG	SYN	RST	FIN ☺←	ACK ☺←

Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 7 – 9

Bienvenido al Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 7 - 9.

Esta evaluación cubre los conceptos básicos y las habilidades presentadas en los Módulos 7 a 9 del curso Dispositivos de Red y Configuración Inicial.

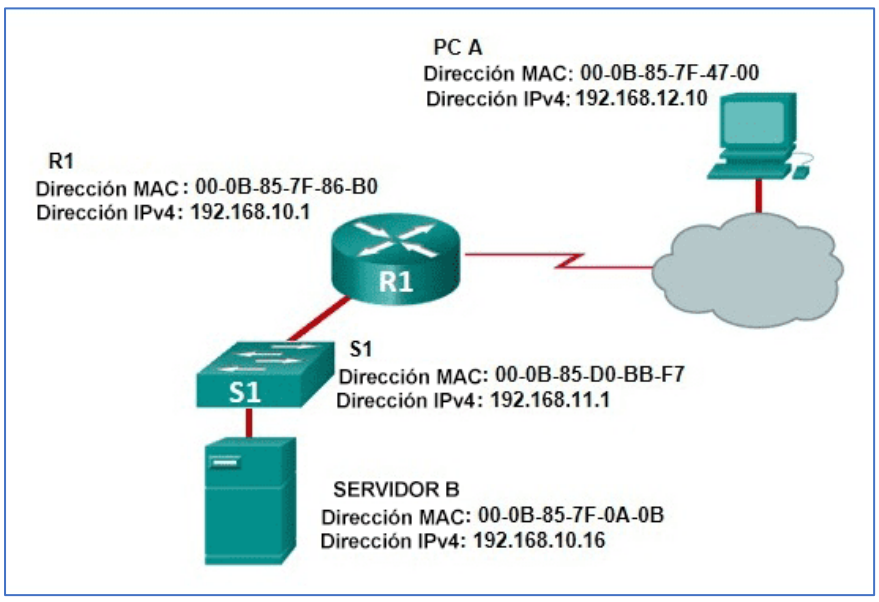
Hay 21 preguntas en total. Debe alcanzar el 70% para aprobar este examen.

Tiene intentos ilimitados para aprobar el examen. Se proporcionan comentarios para dirigirlo a áreas que pueden requerir atención adicional.

El contenido de Cisco Networking Academy está protegido por leyes de derechos de autor y está prohibido publicar, distribuir o compartir el contenido de este examen sin autorización.

© 2022, Cisco Systems, Inc.

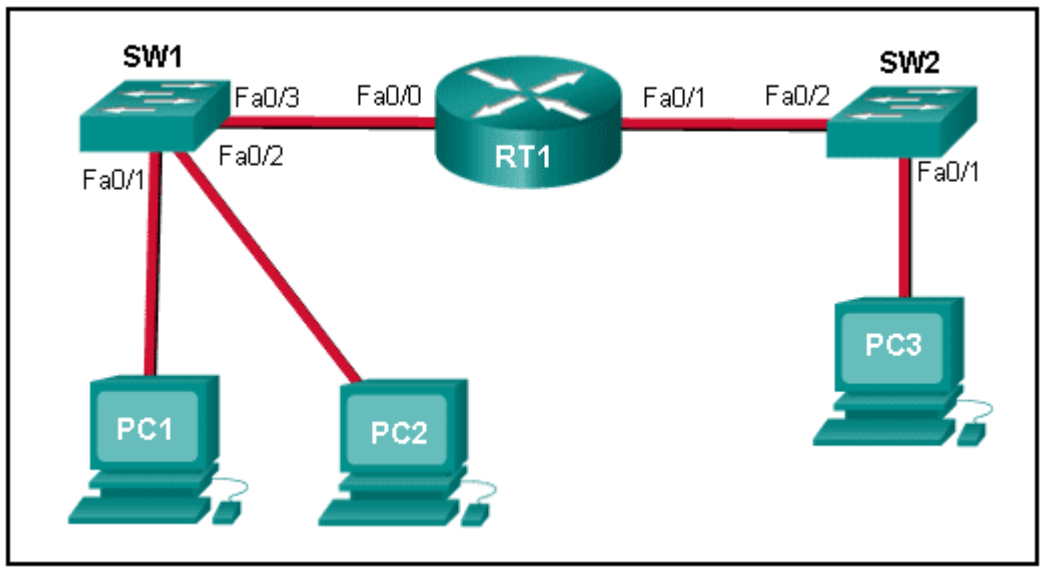
Observe la ilustración. ¿Qué usa R1 como la dirección MAC de destino al construir la trama que irá de R1 al servidor B?



El paquete se encapsula en una trama PPP, y R1 agrega la dirección de destino de PPP a la trama.
Si la dirección MAC de destino que corresponde a la dirección IPv4 no aparece en la caché ARP, R1 envía una solicitud de ARP. ☺←
El R1 utiliza la dirección MAC de destino del S1.
El R1 deja el campo en blanco y reenvía los datos a la PC.

Explique: *La comunicación dentro de la red local usa el protocolo de resolución de direcciones para obtener una dirección MAC de la dirección IPv4 conocida. Se necesita la dirección MAC para construir una trama donde encapsular el paquete.*

Observe la ilustración. PC1 emite una solicitud ARP porque necesita enviar un paquete a PC3. En este escenario, ¿qué pasará a continuación?



RT1 reenviará la solicitud ARP a PC3.
RT1 enviará una respuesta ARP con su propia dirección MAC Fa0/1.
RT1 enviará una respuesta ARP con la dirección MAC de PC3.
RT1 enviará una respuesta ARP con su propia dirección MAC Fa0/0. ☺←
SW1 enviará una respuesta ARP con su dirección MAC Fa0/1.

Explique: *Cuando un dispositivo de red tiene que comunicarse con un dispositivo en otra red, transmite una solicitud ARP solicitando la dirección MAC de la puerta de enlace predeterminada. El gateway predeterminado (RT1) envía una respuesta unicast ARP con la dirección MAC Fa0/0.*

¿Qué enunciado describe la función del Protocolo de Resolución de Direcciones?

ARP se utiliza para detectar la dirección MAC de cualquier host en la red local. ☺←
ARP se utiliza para detectar la dirección IP de cualquier host en la red local.
ARP se utiliza para detectar la dirección MAC de cualquier host en una red diferente.
ARP se utiliza para detectar la dirección IP de cualquier host en una red diferente.

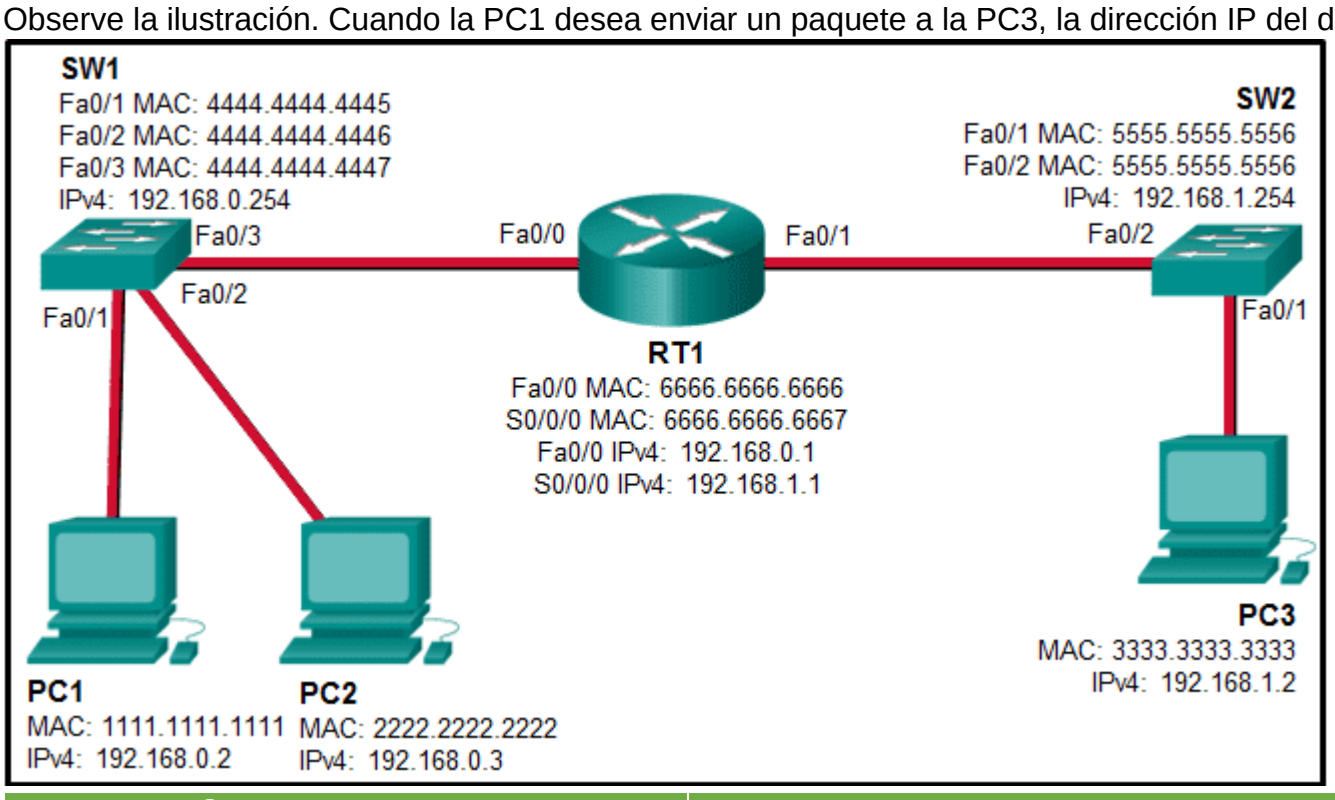
¿Cuál es el protocolo que se utiliza para detectar una dirección física a partir de una dirección lógica conocida y qué tipo de mensaje utiliza?

DNS, difusión	PING, multidifusión
ARP, multidifusión	ARP, difusión ☺←
PING, difusión	DNS, unidifusión

Cuando una computadora hace ping a otra computadora por primera vez, ¿qué tipo de mensaje coloca en la red para determinar la dirección MAC del otro dispositivo?

una multidifusión a cualquier dispositivo de capa 3 que esté conectado a la red local	una solicitud de ARP ☺←
un mensaje RFI (Solicitud de Información)	un ping ICMP

Observe la ilustración. Cuando la PC1 desea enviar un paquete a la PC3, la dirección IP del dispositivo que responderá a la solicitud ARP es



192.168.0.1 ☺←		192.168.1.2	192.168.0.3
192.168.0.2	192.168.1.1	192.168.0.254	192.168.1.254

Un usuario envía una solicitud HTTP a un servidor Web en una red remota. Durante la encapsulación para esta solicitud, ¿qué información se agrega al campo de dirección de una trama para indicar el destino?

La dirección MAC del gateway predeterminado ☺←	El dominio de red del host de destino
La dirección IP de la puerta de enlace predeterminada	La dirección MAC del host de destino

¿Cuáles son las dos tareas que puede realizar un servidor DNS local? (Elija dos opciones).

Proporcionar direcciones IP a los hosts locales.	Reenviar solicitudes de resolución de nombres entre servidores. ☺←
Recuperar mensajes de correo electrónico.	Asignar nombres a direcciones IP para los hosts internos. ☺←
Permitir la transferencia de datos entre dos dispositivos de red.	

¿Qué dos comandos se pueden utilizar para verificar si la resolución de nombres DNS funciona correctamente en un equipo Windows? (Elija dos opciones).

ipconfig /flushdns	ping cisco.com ☺←	nslookup cisco.com ☺←	net cisco.com	netstat cisco.com

¿Qué mensaje DHCP IPv4 contiene la siguiente información?
Dirección de destino: 255.255.255.255
Dirección IPv4 del cliente: 0.0.0.0
Dirección de puerta de enlace predeterminada: 0.0.0.0
Máscara de subred: 0.0.0.0

DHCPREQUEST	DHCPDISCOVER ☺←	DHCPOFFER	DHCPACK

¿Cuáles tres afirmaciones describen un mensaje de detección de DHCP? (Elija tres opciones).

Solo el servidor DHCP recibe el mensaje.
La dirección MAC de origen es de 48 unidades (FF-FF-FF-FF-FF-FF).
La dirección IP destino es 255.255.255.255 ☺←
Todos los hosts reciben el mensaje, pero solo un servidor DHCP responde. ☺←
El mensaje proviene de un servidor que ofrece una dirección IP.
El mensaje proviene de un cliente que busca una dirección IP. ☺←

¿Qué tipo de registro DNS relacionado con IPv4 es utilizado por un servidor DNS en respuesta a un host que solicita una dirección de servidor web a través de la URL?

Registro NS	Registro A ☺←
Registro MX	Registro AAAA

Un usuario informa que no se puede acceder al servidor web corporativo. Un técnico verifica que puede acceder mediante su dirección IP. ¿Cuáles son dos posibles causas del problema? (Elija dos opciones).

La dirección de gateway predeterminado está mal configurada en la estación de trabajo.
La dirección del servidor DNS está mal configurada en la estación de trabajo. ☺←
El servidor web está mal configurado.
La información del servidor web está mal configurada en el servidor DNS. ☺←
No hay conexión a la red.

Se inicia una PC configurada para DHCP. ¿Cuál es el orden de los mensajes que envía y recibe esta PC para obtener una dirección IP adecuada?

DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK	DHCPOFFER, DHCPDISCOVER, DHCPREQUEST, DHCPACK
DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK ☺←	DHCPREQUEST, DHCPOFFER, DHCPDISCOVER, DHCPACK

¿Cuáles dos campos de encabezado TCP se utilizan para confirmar la recepción de datos? (Elija dos opciones).

preámbulo	FCS	número de reconocimiento ☺←	Número de secuencia ☺←	Suma de comprobación

¿Qué mecanismo de TCP se utiliza para mejorar el rendimiento al permitir que un dispositivo envíe continuamente un flujo constante de segmentos siempre que el dispositivo también reciba los reconocimientos necesarios?

Protocolo de enlace de tres vías	Par de sockets
Protocolo de enlace de dos vías	Ventana deslizante ☺←

Explique: *TCP utiliza ventanas para intentar administrar la velocidad de transmisión al flujo máximo que la red y el dispositivo de destino pueden soportar mientras minimiza la pérdida y las retransmisiones. Cuando está saturado de datos, el destino puede enviar una solicitud para reducir el tamaño de la ventana. El proceso en el que el destino envía reconocimientos a medida que procesa los bytes recibidos y el ajuste continuo de la ventana de envío del origen se conoce como ventanas deslizantes.*

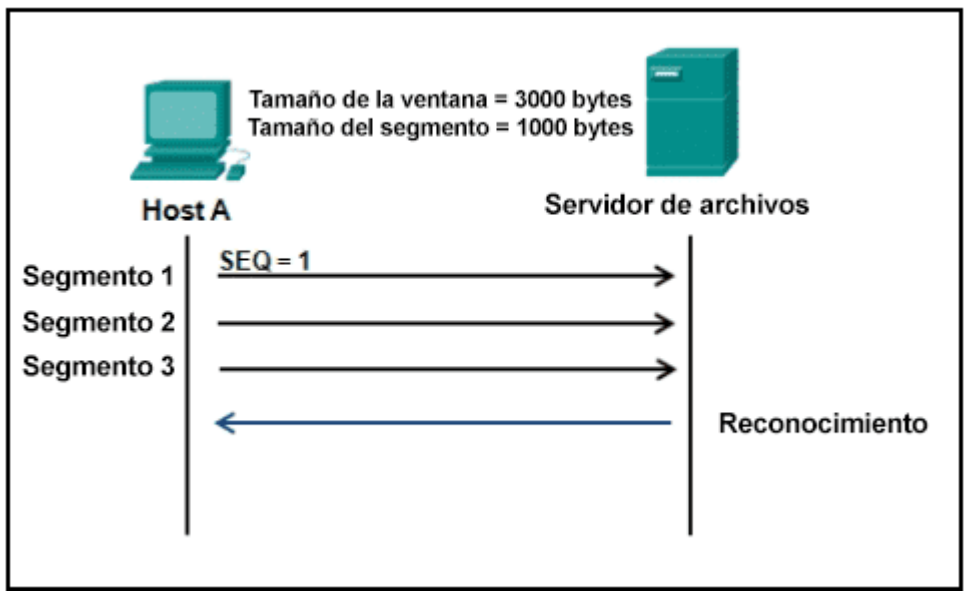
Un dispositivo host debe enviar un archivo de video grande a través de la red mientras proporciona comunicación de datos a otros usuarios. ¿Qué función permitirá que se produzcan diferentes flujos de comunicación al mismo tiempo, sin tener un solo flujo de datos que utilice todo el ancho de banda disponible?

tamaño de ventana	números de puerto	Multiplexación ☺←	Acuses de recibo

¿Qué selecciona una aplicación cliente para un número de puerto de origen TCP o UDP?

un valor predefinido en el rango de los puertos registrados	un valor aleatorio en el rango de puertos bien conocidos
un valor aleatorio en el rango de los puertos registrados ☺←	un valor predefinido en el rango de puertos conocido

Observe la ilustración. El host A y el servidor de archivos han establecido una sesión TCP para intercambiar datos. ¿Qué número de confirmación enviará el servidor de archivos al host A para confirmar la recepción de los primeros tres segmentos de datos?



4000	3000	1002	1000	3001 ☺←

Explique: *El servidor de archivos devolverá un número de acuse de recibo 3001 al host A después de recibir los primeros tres segmentos. El número de secuencia inicial era 1. Se enviaron 1000 bytes en cada uno de los tres segmentos para un total de 3000 bytes. Como el número de secuencia inicial era 1, el último byte enviado fue el número de byte 3000. El servidor de archivos ahora esperará recibir el número de byte 3001 y superiores. Por lo tanto, se comunica con el host A a través del número de acuse de recibo 3001.*

¿Qué es un socket?

- la combinación de la dirección IP de origen y destino y la dirección Ethernet de origen y destino
- la combinación de la secuencia de origen y destino y los números de acuse de recibo
- La combinación de una dirección IP de origen y un número de puerto o una dirección IP de destino y un número de puerto ☺←
- La combinación de los números de secuencia de origen y destino y los números de puerto

Un cliente está estableciendo una sesión TCP con un servidor. ¿Cómo se determina el número de reconocimiento en el segmento de respuesta al cliente?

- El campo de número de reconocimiento utiliza un número de puerto de origen aleatorio en respuesta al cliente.
- El número de reconocimiento se establece en 11 para indicar un paquete de reconocimiento y un paquete de sincronización al cliente.
- El número de reconocimiento se establece en 1 para indicar un paquete de reconocimiento al cliente.
- El campo de número de reconocimiento se modifica agregando 1 al número de secuencia inicial elegido aleatoriamente en respuesta al cliente. ☺←

Modulo 10: La Línea de Comandos del IOS de Cisco

0. Introducción

10.0.1 Webster - ¿Por Qué Debería Tomar este Módulo?

Hola, Tengo otro amigo que quiero que conozcas. Diego acaba de ser contratado como miembro junior de un nuevo departamento de TI para una pequeña empresa de fabricación en Cuzco, Perú. Esta empresa crea piezas para equipos agrícolas y de molienda. Recientemente han actualizado y ampliado sus operaciones. Necesitan una red en la segunda ubicación que esté conectada a su nueva red en la sede central. La mayor parte del equipo está fabricado por Cisco, por lo que Diego debe aprender rápidamente las funciones de la línea de comandos del IOS de Cisco. Afortunadamente, hay ayuda y Diego estará listo en poco tiempo. ¿Y usted? Si desea obtener información sobre las funciones de la línea de comandos del IOS de Cisco, este módulo es para usted.

10.0.2 ¿Qué Voy a Aprender en este Módulo?

Título del Módulo: La Línea de Comandos del IOS de Cisco

Objetivo del Módulo: Utilizar el IOS de Cisco.

Título del Tema	Objetivo del Tema
Navegación IOS	Utilice los comandos correctos para navegar por los modos del IOS de Cisco.
La Estructura de Comandos	Explicar la forma en que se explora el IOS de Cisco para configurar los dispositivos de red.
Ver la Información del Dispositivo	Use los comandos show para monitorear las operaciones del dispositivo.

1. Navegación del IOS

10.1.1 La Interfaz de Línea de Comandos del IOS de Cisco

La interfaz de línea de comandos (CLI) del IOS de Cisco es un programa basado en texto que permite el ingreso y ejecución de comandos para configurar, monitorear y mantener los dispositivos de Cisco. La CLI de Cisco puede ser utilizada para tareas de administración tanto ***dentro de banda*** como ***fuera de banda.***

Utilice los comandos de la CLI para modificar la configuración del dispositivo y para mostrar el estado actual de los procesos del enrutador. Para los usuarios avanzados, la CLI ofrece muchas características que sirven para ahorrar tiempo al crear configuraciones simples y complejas. Casi todos los dispositivos de red Cisco utilizan una CLI similar. Cuando el enrutador ha completado la secuencia de encendido y aparece el indicador **Router>**, se puede utilizar la CLI para ingresar los comandos IOS de Cisco, como se muestra en la salida del comando.

```
Router con0 is now available


Press RETURN to get started!



Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)#
```

A los técnicos que están familiarizados con los comandos de IOS y con el funcionamiento de la CLI les resulta fácil monitorear y configurar una variedad de distintos dispositivos de red porque se usan los mismos comandos básicos para configurar un conmutador y un enrutador. La CLI cuenta con un amplio sistema de ayuda que asiste a los usuarios en la configuración y el monitoreo de los dispositivos.

10.1.2 Modos de Comando Principales

Todos los dispositivos de red requieren un sistema operativo y pueden configurarse mediante la CLI o una GUI. El uso de la CLI puede proporcionar al administrador de red un control y flexibilidad más precisos que el uso de la GUI. En este tema se describe el uso de CLI para navegar por Cisco IOS. Como característica de seguridad, el software IOS de Cisco divide el acceso de administración en los siguientes dos ***modos de comando***:

- **Modo EXEC usuario** - Este modo tiene capacidades limitadas, pero resulta útil en el caso de algunas operaciones básicas. Permite solo una cantidad limitada de comandos de monitoreo básicos, pero no permite la ejecución de ningún comando que podría cambiar la configuración del dispositivo. El modo EXEC usuario se puede reconocer por la petición de entrada **(*prompt*)** de la CLI que termina con el símbolo **>**.
- **Modo EXEC privilegiado**- Para ejecutar comandos de configuración, un administrador de redes debe acceder al modo EXEC privilegiado. Solo se puede ingresar al ***modo de configuración global*** y a los modos de configuración más altos por medio del modo EXEC privilegiado, se puede reconocer por la petición de entrada que termina con el símbolo **#**.

Modo de Comando	Descripción	Indicador predeterminado del dispositivo
Usuario	Permite el acceso solo a una cantidad limitada de comandos básicos de monitoreo. Conocido como modo de “visualización solamente”.	Switch> Router>
Privilegiado	Permite el acceso a todos los comandos y funciones. El usuario puede utilizar cualquier comando de monitoreo y ejecutar comandos de configuración y de administración.	Switch# Router#

10.1.3 Video - Modos de Comando Principales de la CLI del IOS

Examinemos los modos de comando de Cisco IOS. Haré clic en PC1, clic en el ***programa de emulación de terminal***, clic en Aceptar y podrá ver que se me presenta una interfaz de línea de comandos de la consola. Este es Cisco IOS. Presionaré enter en mi teclado para comenzar. Observe el símbolo del sistema en la parte inferior izquierda de la pantalla que indica el modo de comando en el que estoy. Cisco IOS utiliza diferentes modos de comando para establecer varios niveles de privilegios para los usuarios. Hay diferentes comandos disponibles en cada modo, por ejemplo, **“>”** indica que estoy en modo ***EXEC usuario***. Este modo tiene muy pocos privilegios, con acceso solo a un número limitado de comandos. Uno de esos comandos disponibles en este modo es el comando **enable** (habilitar). En el cursor parpadeante, escribiré el comando **enable** y presionaré Intro, y ahora estoy en modo ***EXEC con privilegios***. Me doy cuenta de esto porque el prompt ha cambiado de **>** a # (hash o almohadilla). El modo de ejecución privilegiado ofrece más comandos disponibles. Si quisiera ir a un nivel de privilegios más alto, puedo entrar en el ***modo de configuración global***. Puedo acceder al modo de configuración global escribiendo ***configure terminal*** y presionando enter. Y ahora puede ver el prompt **(config)#**. Aquí es donde se realizan la mayoría de las configuraciones de un conmutador o enrutador. También hay otros modos de configuración como el ***modo de configuración de interfaz***. Si escribo ***interface vlan 1*** y presiono enter, aparece un prompt indicando **(config-if)#**. Muchos comandos solo funcionarán desde ciertos modos. Un error común que cometen los usuarios nuevos en el trabajo con Cisco IOS es tratar de usar comandos desde el modo incorrecto. Si está seguro de que está escribiendo un comando correctamente, pero recibe continuamente un mensaje de error, verifique siempre el prompt para asegurarse de que está en el modo correcto.

```
Switch   Ports  Model              SW Version            SW Image
------   -----  -----              ----------            ----------
*    1   26     WS-C2960-24TT      12.2                  C2960-LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTW
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#
```

10.1.4 Video - Navegando Entre los Modos del IOS

Veamos los comandos que se utilizan para moverse en iOS. Veremos el comando ***enable, disable, configure terminal, exit, end, Ctrl z***, además de algunos comandos para ingresar a diferentes modos de sub configuración. Tengo una conexión de consola a Switch, haré clic en PC 1, presionaré Intro y me lleva al modo de EXEC usuario. Para ingresar al modo EXEC privilegiado, escribo ***enable***. Si quiero volver al modo EXEC de usuario, puedo escribir ***disable***. Escribiré enable para volver al modo EXEC privilegiado. Para configurar el conmutador, primero debo acceder al modo de configuración global, escribiré ***configure terminal*****,** puede ver que ahora estoy en el prompt de configuración global. Puedo escribir ***exit*** y presionar enter para volver al modo EXEC privilegiado. Si vuelvo a escribir **exit**, dejo la conexión de mi consola por completo para volver a ingresar al Switch y obtener una interfaz de línea de comando. Tengo que presionar enter en mi teclado y ahora vuelvo a la conexión de la consola con el interruptor. Escribiré ***enable*** y presiono enter y luego ***config t*** (abreviatura de ***configure terminal***) y ahora estoy de regreso en modo de configuración global. Ingresemos a uno de los modos de subconfiguración, escribiré ***line console 0*** para llegar a la interfaz de administración del puerto de la consola. Ahora que estoy en un modo de subconfiguración, escribo ***exit*** y regreso al modo de configuración global. Esta vez escribiré ***line vty 0 15*** para las interfaces de administración de terminal virtual. Estos se utilizan para el acceso administrativo remoto al Switch. Puedo pasar directamente de un modo de subconfiguración a otro. Escribo ***interface vlan 1*** y presiono enter, el prompt cambia del modo de configuración de línea al modo de configuración de interfaz. Desde aquí también puedo ingresar a diferentes interfaces como la Fast Ethernet 0/1 escribiendo ***interface fastethernet 0/1***. También puedo pasar directamente a la consola de línea 0 (**line console 0**). Los comandos que normalmente se ejecutan en el modo de configuración global también se pueden ejecutar desde cualquiera de los modos de subconfiguración. Si quiero salir de todos los modos de subconfiguración y volver al modo EXEC privilegiado, puedo usar el comando ***end*** o presionar ***Ctrl+Z***, enter, y ahora puede ver que he regresado al modo EXEC privilegiado. Si estoy en modo de configuración global, escribo **end** y presiono Enter, también vuelvo al modo EXEC privilegiado. Aprender a navegar eficientemente entre los diferentes modos de comando le ahorrará mucho tiempo.

```
Switch1(config-line)#exit
Switch1(config)#line vty 0 15
Switch1(config-line)#interface vlan 1
Switch1(config-if)#interface fastethernet 0/1
Switch1(config-if)#line console 0
Switch1(config-line)#end
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#line console 0
Switch1(config-line)#^Z
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#end
Switch1#
%SYS-5-CONFIG_I: Configured from console by console
```

10.1.5 Una Nota Sobre las Actividades del Verificador de Sintaxis

Cuando esté aprendiendo a modificar las configuraciones de los dispositivos, es posible que desee comenzar en un entorno seguro que no sea de producción antes de probarlo en equipos reales. Hay diferentes herramientas de simulación para ayudarlo a desarrollar sus habilidades de configuración y resolución de problemas. Debido a que se trata de herramientas de simulación, normalmente no tienen toda la funcionalidad del equipo real. Una de esas herramientas es el ***Verificador de Sintaxis***. En cada Verificador de Sintaxis, se le da un conjunto de instrucciones para introducir un conjunto específico de comandos. No puede progresar en el Verificador de Sintaxis a menos que se introduzca el comando exacto y completo como se especifica. Las herramientas de simulación más avanzadas, como ***Packet Tracer***, le permiten introducir comandos abreviados, como lo haría con equipos reales.

10.1.6 Verificador de Sintaxis - Navegar entre los Modos IOS

```
Switch(config)# interface vlan 1
```

Desde el modo de configuración de interfaz, cambie al modo de subconfiguración de la consola de línea mediante el comando de configuración **line console 0** global.

```
Switch(config-if)# line console 0
```

Regrese al modo EXEC privilegiado utilizando el comando. **end**

```
Switch(config-line)# end
```

Ha navegado correctamente entre los distintos modos de línea de comandos del IOS.

Restablecer | Mostrar | Mostrar todo

10.1.7 Verifique su Comprensión - Navegación del IOS

¿Qué modo IOS permite el acceso a todos los comandos y funciones?

modo de configuración global	modo de subconfiguración de la interfaz
modo de subconfiguración de la línea de consola	modo EXEC privilegiado ☺←
modo EXEC del usuario	

¿En qué modo IOS se encuentra si se muestra el indicador Switch(config)#?

modo de configuración global ☺←	modo de subconfiguración de la interfaz
modo de subconfiguración de la línea de consola	modo EXEC privilegiado
modo EXEC del usuario	

¿En qué modo IOS se encuentra si se muestra el símbolo del switch>?

modo de configuración global	modo de subconfiguración de la interfaz
modo de subconfiguración de la línea de consola	modo EXEC privilegiado
modo EXEC del usuario ☺←	

¿Qué dos comandos le devolverían al símbolo EXEC privilegiado independientemente del modo de configuración en el que se encuentre? (Elija dos opciones).

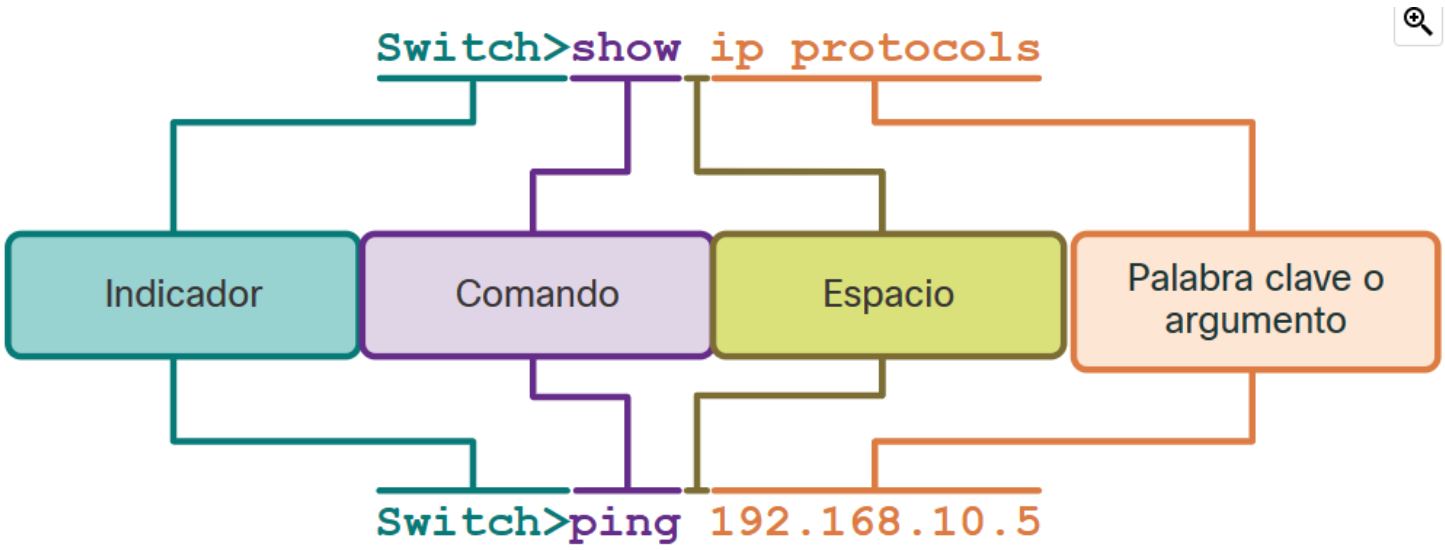
Ctrl Z ☺←	disable	enable	End ☺←	exit

2. La estructura de comandos

10.2.1 Estructura Básica de los Comandos de IOS

Un administrador de red debe conocer la estructura de comandos básica del IOS para poder usar la CLI para la configuración del dispositivo.

Los dispositivos Cisco IOS admiten muchos comandos. Cada comando de IOS tiene una sintaxis o formato específico y puede ejecutarse solamente en el modo adecuado. La sintaxis general para un comando, que se muestra en la figura, es el comando seguido de cualquier palabra clave y argumento apropiados.



- **Palabra clave** - Este es un parámetro específico que se define en el sistema operativo (en la figura, **ip protocols**)
- **Argumento** - No está predefinido; es un valor o variable definido por el usuario, (en la figura, **192.168.10.5**)

Después de ingresar cada comando completo, incluso cualquier palabra clave y argumento, presione la tecla **Enter** (Introducir) para enviar el comando al intérprete de comandos.

10.2.2 Sintaxis de los Comandos de IOS

Un comando podría requerir uno o más argumentos. Para determinar cuáles son las palabras clave y los argumentos requeridos para un comando, consulte la sintaxis de comandos. La sintaxis proporciona el patrón o el formato que se debe utilizar cuando se introduce un comando.

Como se identifica en la tabla, el texto en negrita indica los comandos y las palabras clave que se ingresan como se muestra. El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.

Convención	Descripción
negrita	El texto en negrita indica los comandos y las palabras clave que se introducen literalmente como se muestran.
cursiva	El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.
[x]	Los corchetes indican un elemento opcional (palabra clave o argumento)
{ x }	Las llaves indican un elemento obligatorio (palabra clave o argumento)
[x { y | z }]	Las llaves y las líneas verticales dentro de corchetes indican una opción obligatoria dentro de un elemento opcional. Los espacios se utilizan para delinear claramente partes del comando.

Por ejemplo, la sintaxis para utilizar el comando **description** es **description** *caracteres.* El argumento en *caracteres* es un valor proporcionado por el usuario. El comando **description** suele utilizarse para identificar el propósito de una interfaz. Por ejemplo, cuando se ingresa el comando, **description Conecta al conmutador principal de la oficina central**, describe la ubicación del otro dispositivo al otro extremo de la conexión. Los siguientes ejemplos muestran algunas convenciones utilizadas para registrar y usar comandos de IOS:

- **ping** *dirección-ip* - El comando es **ping** y el argumento definido por el usuario *dirección-ip* es la dirección IP del dispositivo de destino. Por ejemplo, **ping 10.10.10.5**.
- **traceroute** *dirección-ip* - El comando es **traceroute** y el argumento *dirección-ip* definido por el usuario es la dirección IP del dispositivo de destino. Por ejemplo, **traceroute 192.168.254.254**.

Si un comando es complejo con múltiples argumentos, puede verlo representado así:

```
Switch(config-if)# switchport port-security aging { static | time time | type
{absolute | inactivity}}
```

Por lo general, el comando irá seguido de una descripción detallada del comando y cada argumento en la Referencia de Comandos de Cisco IOS.

La referencia de comando de Cisco IOS es la última fuente de información para un comando de IOS en particular.

10.2.3 Video - Ayuda Sensible al Contexto y Verificación de Sintaxis de Comandos

Se accede al ***comando ayuda*** de Cisco IOS mediante el signo de interrogación (**?**). El comando ayuda es sensible al contexto, por lo que importa cómo y dónde se use. Si quiero una lista de todos los comandos disponibles en el modo usuario simplemente escribo **?.** Si escribo ***enable*** ingreso al modo EXEC privilegiado, pongo **?** y me da los comandos disponibles en este modo. Presiono la ***barra espaciadora*** para obtener la siguiente página de salida, incluso hay diferentes comandos disponibles para usuario pero en el modo configuración global. También hay otros usos para el ***comando ayuda***. Digamos que no quiero una lista de todos los comandos disponibles y solo quiero ayuda para encontrar un comando en particular, por ejemplo digamos que estoy instalando la interfaz de comandos, pero olvidé cuál es el nombre completo del comando. He escrito **in** y necesito ayuda para terminar el comando, pongo parte del comando y luego el signo **?** me ayudará a terminar el comando. Observe que puse **in** y luego un signo de interrogación y el comando de ayuda lo devolvió. El comando que estoy buscando es **interface**. El comando de ayuda puede usarse también en otro contexto. Entonces, ahora que sé que el comando es **interface**, digamos que no estoy seguro de cuál es el siguiente parámetro o argumento del comando. En este caso, pondré un espacio y luego un signo de interrogación y me dirá el siguiente parámetro o argumento que requiere el comando **interface**. Ahora sé que la siguiente parte del comando es el nombre de la interfaz, como Ethernet, Fast Ethernet, Gigabit Ethernet, o quizás sea Vlan o range. Relacionado con el comando de ayuda está el verificador de sintaxis del comando. El comando me avisará cuando tenga un problema con el comando que ingresé. Por ejemplo, podemos ver aquí que la siguiente parte de este comando sería uno de estos argumentos aquí. Digamos que hago un error y escribo el número 33 en lugar de VLAN o range y presiono Intro. Observe que el Comprobador de sintaxis del comando me ha informado que, comenzando en el número tres, he realizado una entrada no válida. Esto es extremadamente útil porque me ayuda a aislar dónde está el problema con el comando particular que ejecuto en ese momento. Esto también puede funcionar en diferentes contextos. Por ejemplo, digamos que ingresé solo la letra “i” en lugar de **interface** y presioné enter. El Comprobador de sintaxis de comandos me informa que la letra “i” es un comando ambiguo, ya que si escribo “i?”, en realidad hay dos comandos “ip” e **interface** en el modo de configuración global. El tercer ejemplo del Comprobador de sintaxis de comandos es cuando escribo interface y presiono Intro. El Comprobador de sintaxis de comandos me ha informado que el comando está incompleto. Para resolver esto, pongo **interface ?** y recibo el siguiente conjunto de opciones que necesito para terminar este comando. Puede ver cómo el comando de ayuda es muy útil para aprender los diferentes comandos que están disponibles para usted, así como el contexto correcto y el uso de los diferentes comandos.

```
  privilege           Command privilege parameters
  service             Modify use of network based services
  snmp-server         Modify SNMP engine parameters
  spanning-tree       Spanning Tree Subsystem
  username            Establish User Name Authentication
  vlan                Vlan commands
  vtp                 Configure global VTP state
Switch(config)#in?
interface
Switch(config)#interface ?
  Ethernet          IEEE 802.3
  FastEthernet      FastEthernet IEEE 802.3
  GigabitEthernet   GigabitEthernet IEEE 802.3z
  Port-channel      Ethernet Channel of interfaces
  Vlan              Catalyst Vlans
  range             interface range command
Switch(config)#interface
```

10.2.4 Teclas de Acceso Rápido y de Método Abreviado

La CLI de IOS proporciona teclas de acceso rápido y accesos directos que facilitan la configuración, el monitoreo y la solución de problemas.

Los comandos y las palabras clave pueden acortarse a la cantidad mínima de caracteres que identifica a una selección única. Por ejemplo, el comando ***configure*** puede acortarse a ***conf***, ya que ***configure*** es el único comando que empieza con ***conf***. Una versión más corta, como ***con***, no dará resultado, ya que hay más de un comando que empieza con ***con***. Las palabras clave también pueden acortarse.

Pulsar teclas	Descripción
Tabulación	Completa una entrada de nombre de comando parcial
Retroceso	Borra el carácter a la izquierda del cursor
Ctrl+D	Borra el carácter donde está el cursor
Ctrl+K	Borra todos los caracteres desde el cursor hasta el final de la línea de comandos
Esc D	Borra todos los caracteres desde el cursor hasta el final de la palabra
Ctrl+U o Ctrl+X	Borra todos los caracteres desde el cursor hasta el comienzo de la línea de comandos
Ctrl+W	Borra la palabra a la izquierda del cursor
Ctrl+A	Desplaza el cursor hacia el principio de la línea
Flecha Izquierda o Ctrl+B	Desplaza el cursor un carácter hacia la izquierda
Esc B	Desplaza el cursor una palabra hacia la izquierda
Esc F	Desplaza el cursor una palabra hacia la derecha
Ctrl+F o Flecha Derecha	Desplaza el cursor un carácter hacia la derecha
Ctrl+E	Desplaza el cursor hacia el final de la línea de comandos
Ctrl+P o Flecha Arriba	Recupera el comando anterior en el historial del búfer, comenzando con el comando mas reciente
Ctrl+N o Flecha Abajo	Va a la línea siguiente en el historial del búfer
Ctrl+R, Ctrl+I o Ctrl+L	Vuelve a mostrar la petición de entrada del sistema y la línea de comando después que se recibe un mensaje de la consola

Nota: Si bien la tecla **Suprimir** generalmente elimina el carácter a la derecha del indicador, la estructura de comandos de IOS no reconoce la tecla **Suprimir**.

Cuando una salida de comando produce más texto del que se puede mostrar en una ventana de terminal, el IOS mostrará un mensaje **«—More—»**. En la tabla siguiente se describen las pulsaciones de teclas que se pueden utilizar cuando se muestra esta solicitud.

Pulsación de teclas	Descripción
Entrar	Muestra la siguiente línea.
Espacio	Muestra la siguiente pantalla.
Cualquier otra tecla*	Finaliza la cadena de visualización y vuelve al indicador anterior. *Excepto "y", que responde "sí" al indicador --**More**-- y actúa como el **Espacio**.

En esta tabla se enumeran los comandos utilizados para salir de una operación.

Pulsación de teclas	Descripción
Ctrl-C	Cuando está en cualquier modo de configuración, termina el modo de configuración y regresa al modo EXEC privilegiado. Cuando está en modo de configuración, interrumpe y regresa al símbolo del sistema.
Ctrl-Z	Cuando está en cualquier modo de configuración, termina el modo de configuración y regresa al modo EXEC privilegiado.
Ctrl-Shift-6	Secuencia de interrupción multipropósito utilizada para cancelar búsquedas de DNS, rastrear rutas, hacer ping y para interrumpir un proceso de IOS.

10.2.5 Video - Teclas de Acceso Rápido y Métodos Abreviados

La compatibilidad con teclas de acceso rápido y accesos directos hace que Cisco IOS sea extremadamente eficiente, su uso le ahorrará mucho tiempo cuando esté configurando dispositivos. Tengo una conexión de consola a un conmutador, en lugar de usar el programa de emulación de terminal para consola, haré clic directamente en el Switch e iré a la pestaña CLI. Al presionar Intro, me llevará a la interfaz de línea de comandos. Este es un acceso directo a CLI disponible dentro del rastreador de paquetes. La primera tecla de acceso rápido de la que hablaré es la tecla de tabulación para completar automáticamente los comandos. Para acceder al modo EXEC privilegiado, normalmente escribiría el comando ***enable***. Con ***tab*** simplemente escriba las primeras letras del comando, en este caso ***en,*** presiono la tecla de tabulación y el comando se completará automáticamente. Si quiero poner el comando ***configure*** para configurar terminal y escribo ***con*** y presiono tabulador, no funciona ya que el comando no está completo. Eso es porque si pongo un signo de interrogación, puede ver que hay más de un comando que comienza con las letras ***con*** en modo ejecutivo privilegiado. Si quiero usar la finalización de tabulación, tendré que escribir ***conf*** y presionar la tecla de tabulación y ahora puede ver que el comando está completo. Para la palabra ***terminal***, todo lo que tengo que hacer es escribir la letra ***t*** y presionar la tecla de tabulación ya que hay solo un argumento o comando secundario que sigue a ***configure*** y comienza con la letra ***t***, para que el switch sepa que el comando que quiero es ***terminal***. Incluso mejor que usar la tecla de tabulación es acortar comandos, o sea en lugar de presionar la tecla de tabulación para completar el comando, simplemente usa las primeras letras del comando y el iOS aceptará el comando abreviado sin presionar la tecla de tabulación. Esto es extremadamente útil, por ejemplo, en lugar de escribir el comando **interface Fast Ethernet 0/1**, que es un comando muy largo, escriba **int f 0/1** y presione enter, el IOS reconoce automáticamente el comando que quiero y lo ejecuta. A veces es necesario repetir los comandos, la forma más rápida de hacer esto es recorrer el historial de comandos usando las teclas de flecha hacia arriba y hacia abajo. Si escribo **end** en mi teclado y presiono enter, volveré al modo EXEC privilegiado y luego presiono la tecla de flecha hacia arriba puede ver que hay dos comandos en mi historial de comandos. Presionar la tecla de flecha hacia abajo me llevará hacia adelante mi historial de comandos, esto es muy útil para los comandos que se usan repetidamente. Ahora echemos un vistazo a algunas teclas de acceso rápido. Tanto el ***Ctrl+Z*** como el ***Ctrl+C*** nos llevarán de vuelta al modo ejecutivo privilegiado. Si mantengo presionado ***Ctrl+Z*** y presiono enter puede ver que he vuelto al prompt de EXEC privilegiado. El ***Ctrl+C*** hará lo mismo y también se puede usar para abortar ciertos comandos. Por ejemplo, si escribo **conf t** y luego cambio de opinión, puedo presionar ***Ctrl+C*** y el comando aborta. ***Ctrl+A*** hará que el cursor salte al comienzo de una línea. Escribiré ***configure***, luego presiono ***Ctrl+A*** y veo que el cursor parpadeante ahora está de regreso al comienzo de la línea. Si presiono ***Ctrl+E***, el cursor salta al final de la línea. ***Ctrl+Shift+6*** es otra combinación de teclas útil, esta secuencia interrumpirá la ejecución de un comando después de que el comando ya se haya ingresado. Digamos, por ejemplo, que escribí mal el comando ***configure*** y presioné enter en mi teclado, el iOS está tratando de traducir las letras que escribí en una dirección IP. Entonces, en lugar de quedarme atrapado en esta situación, simplemente puedo presionar ***Ctrl+Shift+6*** y el comando se aborta. Por último, puede haber ocasiones en las que esté trabajando en la CLI de un dispositivo y ocurra un evento que genere un mensaje que interrumpa el comando que está escribiendo. Esto puede ser muy molesto. Si esto ocurre, presione ***Ctrl+R*** en su teclado para regresar al indicador donde se mostrará el comando parcial, lo que le permitirá terminar de escribir. Esta secuencia no se admite actualmente en esta versión de Packet Tracer. Simularé el uso de estas teclas de acceso rápido al consolar en un interruptor físico y apagar una interfaz en el interruptor mientras estoy escribiendo un comando. Presionaré enter y escribiré ***enable*** para poder acceder al modo ejecutivo privilegiado, luego entraré en el modo de configuración global. Digamos que quiero ingresar a la interfaz G0/1. Comenzaré a escribir el comando. Y ahora cerraré una interfaz. Puede ver el mensaje que se muestra en la pantalla. Si simplemente presiono ***Ctrl+R***, vuelvo a donde lo dejé y puedo seguir escribiendo. Eso es genial. El uso de teclas de acceso rápido y accesos directos es una excelente manera de ahorrar tiempo cuando trabaja con Cisco IOS.

```
Switch1>enable
Switch1#con
Switch1#con?
configure  connect
Switch1#conf
Switch1#configure t
Switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#int f 0/1
Switch1(config-if)#end
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#^Z
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#conf t
Switch1#
```

10.2.6 Packet Tracer - Navegar por el IOS

Packet Tracer - Navega por el IOS

Objetivos

Parte 1: Establecer conexiones básicas, acceder a la CLI y explorar la Ayuda

Parte 2: Explorar los modos EXEC

Parte 3: Configurar el reloj (tiempo)

Antecedentes/Escenario

En esta actividad, practicará las habilidades necesarias para navegar dentro de Cisco IOS, tales como los distintos modos de acceso de usuario, diversos modos de configuración y comandos comunes que se utilizan habitualmente. También practicará el acceso a la ayuda contextual mediante la configuración del comando **clock**.

Instrucciones

Parte 1: Establecer conexiones básicas, acceder a la CLI y explorar la ayuda

Paso 1: Conectar la PC1 a S1 mediante un cable de consola.

a. Haga clic en el icono de **conexiones** (el que parece un rayo) en la esquina inferior izquierda de la ventana de Packet Tracer.

b. Haga clic en el cable de consola celeste para seleccionarlo. El puntero del mouse cambia a lo que parece ser un conector con un cable que cuelga de él.

c. Haga clic en **PC1**. Aparece una ventana que muestra una opción para una conexión RS-232. Conecte el cable al puerto RS-232.

d. Arrastre el otro extremo de la conexión de consola al switch S1 (conmutador) y haga clic en el switch para acceder a la lista de conexiones.

e. Seleccione el puerto **Console** para completar la conexión.

Paso 2: Establecer una sesión de terminal con el S1.

a. Haga clic en **PC1** y luego en la pestaña **Desktop**.

b. Haga clic en el ícono de la aplicación **Terminal**. Verifique que los parámetros predeterminados de la configuración de puertos sean correctos.

¿Cuál es el parámetro de bits por segundo? **9600**.

c. Haga clic en **OK**.

d. La pantalla que aparece puede mostrar varios mensajes. En alguna parte de la pantalla tiene que haber un mensaje que diga **Press RETURN to get started!** Presione INTRO (ENTER).

¿Cuál es la petición de entrada que aparece en la pantalla? **S1>**

Paso 3: Examinar la ayuda de IOS.

a. El IOS puede proporcionar ayuda para los comandos según el nivel al que se accede. La petición de entrada que se muestra actualmente se denomina **Modo EXEC del usuario** y el dispositivo está esperando un comando. La forma más básica de solicitar ayuda es escribir un signo de interrogación (?) en la petición de entrada para mostrar una lista de comandos.

S1> **?**

¿Qué comando comienza con la letra “C”? **connect**

b. En el indicador, escriba **t** y luego un signo de interrogación (?).

S1> **t?**

¿Qué comandos se muestran? **telnet terminal traceroute**

En el indicador, escriba **te** y luego un signo de interrogación (?).

S1> **te?**

¿Qué comandos se muestran? **telnet terminal**

Este tipo de ayuda se conoce como ayuda sensible al contexto. Proporciona más información a medida que se expanden los comandos.

Parte 2: Explorar los modos EXEC

En la parte de la actividad, debe cambiar al modo EXEC privilegiado y emitir comandos adicionales.

Paso 1: Ingresar al modo EXEC con privilegios.

a. En la petición de entrada, escriba el signo de interrogación (**?**).

S1> **?**

¿Qué información se muestra para el comando **enable**? **Habilitar comandos con privilegios**

b. Escriba **en** y presione la tecla **Tabulación**.

S1> **en<Tab>**

¿Qué se muestra después de presionar la tecla **Tabulación**? **enable**

Esto se llama finalización de comando (o finalización de tabulación). Cuando se escribe parte de un comando, la tecla **Tab** se puede utilizar para completar el comando parcial. Si los caracteres que se escriben son suficientes para formar un comando único, como en el caso del comando **enable**, se muestra la parte restante.

¿Qué ocurriría si escribiera **te<Tab>** en la petición de entrada?

Hay más de un comando que comienza con las letras "te" porque "te" no proporciona suficientes caracteres para que el comando sea único. Los caracteres continuarán apareciendo, solicitando al usuario caracteres adicionales para que el comando sea único.

c. Introduzca el comando **enable** y presione ENTER.

¿Cómo cambia la petición de entrada? **Cambia de S1> a S1#, que indica el modo EXEC privilegiado.**

d. Cuando se le solicite, escriba el signo de interrogación (**?**).

S1# **?**

Antes había un comando que comenzaba con la letra “C” en el modo EXEC del usuario.

¿Cuántos comandos se muestran ahora que está activo el modo EXEC privilegiado? (**Ayuda**: puede escribir c? para que aparezcan solo los comandos que comienzan con la letra “C”) **5: clear, clock, configure, connect y copy**

Paso 2: Ingresar al modo de configuración global

a. Cuando se encuentra en el modo EXEC privilegiado, uno de los comandos que comienza con la letra “C” es **configure**. Escribe el comando completo o una parte suficiente como para que sea único. Presione la tecla <**Tabulación**> para emitir el comando y presione la tecla ENTER.

S1# **configure**

¿Cuál es el mensaje que se muestra? **Configuring from terminal, memory, or network [terminal]?**

b. Presione Enter para aceptar el parámetro predeterminado que se encuentra entre corchetes **[terminal]**.

¿Cómo cambia la petición de entrada? **S1(config)#**

c. Esto se denomina modo de configuración global. Este modo se analizará en más detalle en las próximas actividades y prácticas de laboratorio. Por el momento, escriba **end**, **exit** o **Ctrl-Z** para volver al modo EXEC privilegiado.

S1(config)# **exit**

S1#

Parte 3: Configuración del reloj

Paso 1: Utilizar el comando clock.

a. Utilice el comando **clock** para explorar en más detalle la ayuda y la sintaxis de comandos. Escriba **show clock** en el indicador EXEC privilegiado.

S1# **show clock**

¿Qué información aparece en pantalla? ¿Cuál es el año que se muestra?

UTC Mon Mar 1 1993 preceded by the hours, minutes, and seconds since the device started. El año es 1993.

b. Use la ayuda contextual y el comando **clock** para configurar la hora del interruptor a la hora actual. Introduzca el comando **clock** y presione la tecla Intro.

S1# **clock<ENTER>**

¿Qué información aparece en pantalla? **% Incomplete command**

c. El mensaje “% Incomplete command” se regresa a IOS. Esto significa que el comando **clock** necesita más parámetros. Cuando se necesita más información, se puede proporcionar ayuda escribiendo un espacio después del comando y el signo de interrogación (?).

S1# **clock ?**

¿Qué información aparece en pantalla? **Set the time and date**

d. Configure el reloj con el comando **clock set**. Proceda por el comando un paso a la vez.

S1# **clock set ?**

¿Qué información se solicita? **hh:mm:ss Current Time**

¿Qué información se habría mostrado si solo se hubiera ingresado el comando clock set y no se hubiera solicitado ayuda con el signo de interrogación? **% Incomplete command**

e. En función de la información solicitada por la emisión del comando **clock set ?**, introduzca las 3:00 p.m. como hora utilizando el formato de 24 horas, esto será 15:00:00. Revise si se necesitan otros parámetros.

S1# **clock set 15:00:00 ?**

El resultado devuelve la solicitud de más información:

<1-31> Day of the month

MONTH Month of the year

f. Intente establecer la fecha en 01/31/2035 con el formato solicitado. Puede ser necesario solicitar ayuda adicional utilizando ayuda sensible al contexto para completar el proceso. Cuando termine, emita el comando **show clock** para mostrar la configuración del reloj. El resultado del comando debe mostrar lo siguiente:

S1# **show clock**

*15:0:4.869 UTC Wed Jan 31 2035

g. Si no pudo lograrlo, pruebe con el siguiente comando para obtener el resultado anterior:

S1# **clock set 15:00:00 31 Jan 2035**

Paso 2: Explorar los mensajes adicionales del comando.

a. El IOS proporciona diversos resultados para los comandos incorrectos o incompletos. Continúe utilizando el comando **clock** para explorar los mensajes adicionales con los que se puede encontrar mientras aprende a utilizar el IOS.

b. Emita los siguientes comandos y grabe los mensajes:

S1# **cl<enter>**

¿Qué información se devolvió? **% Ambiguous command: "cl"**

S1# **clock**

¿Qué información se devolvió? **% Incomplete command.**

S1# **clock set 25:00:00**

¿Qué información se devolvió?

S1# clock set 25:00:00
^
% Invalid input detected at '^' marker.

S1# **clock set 15:00:00 32**

¿Qué información se devolvió?

S1# clock set 15:00:00 32
^
% Invalid input detected at '^' marker.

3. Ver la información del dispositivo

10.3.1 Video - Comandos Show del IOS de Cisco

En este video, vamos a ver algunos de los comandos ***show*** básicos en un enrutador Cisco IOS. Este primer comando es **show running-config**. Lo que este comando muestra es la configuración actual en este enrutador, incluye los comandos configurados. Aquí tenemos el host R1 y el prompt **R1#**. Tenemos una contraseña privilegiada. Aquí está la configuración de la interfaz para Fast Ethernet 0/0 y la dirección IPv4. Desplazamiento abajo podemos ver algunas otras configuraciones en este enrutador. La configuración de la interfaz serial 0/0/0. Aquí la máscara de subred de dirección IPv4. También podemos ver que este enrutador ha sido configurado para usar el protocolo de enrutamiento RIP. El puerto de la consola se ha configurado con una contraseña y también hemos configurado el acceso TELNET del terminal virtual VTY para este dispositivo. El comando **show interfaces** nos mostrará esta información o información similar para todas las interfaces en este enrutador. El comando **show arp** muestra la tabla ARP para este enrutador. En este caso, nos muestra el cable ARP para el puerto FastEthernet 0/0. Si este enrutador tuviera más de un puerto Ethernet, nos mostraría las entradas ARP para cada uno de los puertos Ethernet conectados a este enrutador. El comando **show ip route** muestra la tabla de enrutamiento en este enrutador. La información que mostrará es cualquier interfaz conectada directamente. Podemos ver eso con **C**. Estas son las interfaces en este enrutador donde el enrutador tiene una dirección IPv4 en esa interfaz y se conecta directamente a esa red. También vemos **R** que significa RIP o Routing Information Protocol. RIP es un protocolo de enrutamiento dinámico. El router aprendió de esta ruta dinámicamente de otro enrutador. El comando **show protocols** muestra información, tanto global como específica para cualquiera de nuestras 3 interfaces en capas. El comando **show versión** muestra información sobre el sistema operativo y cierta información de hardware sobre este enrutador. Por ejemplo, muestra la versión del sistema operativo, en este caso 12.4. También muestra información sobre las interfaces en este enrutador, y también otra información como la cantidad de memoria NVRAM y otro tipo de información. Estos comandos y muchos otros se pueden usar para ayudar a verificar y solucionar problemas de operaciones de red. Hay diferentes variaciones para cada uno de estos comandos. A medida que desarrolle más habilidades con el uso del sistema operativo, aprenderá a usar e interpretar la salida de estos show commands.

```
R1# show version

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
R1 uptime is 43 minutes
System returned to ROM by reload at 22:05:12 UTC Sat Jan 5 2008
System image file is "flash:c1841-advipservicesk9-mz.124-10b.bin"

Cisco 1841 (revision 6.0) with 174080K/22528K bytes of memory.
Processor board ID FTX1111W0QF
6 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

10.3.2 Comandos Show

Cisco IOS proporciona comandos para verificar el funcionamiento de interfaces del enrutador y conmutador.

Los comandos ***show*** de la CLI del IOS de Cisco muestran información importante sobre la configuración y el funcionamiento del dispositivo. Los técnicos de red utilizan los comandos ***show*** con frecuencia para ver los archivos de configuración, revisar el estado de los procesos y las interfaces del dispositivo, y verificar el estado de funcionamiento del dispositivo. Se puede mostrar el estado de casi todos los procesos o funciones del enrutador mediante un comando ***show***. Los comandos show de uso común y cuándo usarlos se enumeran en la tabla.

Comando	Se usa para
show running-config	Verifica la configuración y los ajustes actuales
show interfaces	Verifica el estado de las interfaces y muestra cualquier mensaje de error.
show ip interface	Verifica la información de la Capa 3 de una interface
show arp	Verifica la lista de hosts conocidos en las LAN Ethernet locales
show ip route	Verifica la información de enrutamiento de Capa 3
show protocols	Verifica cuales protocolos están operativos
show version	Verifica la memoria, las interfaces y las licencias del dispositivo

Comando ***show running-config*****:** Verifica la configuración y los ajustes actuales

```
R1# show running-config

(Output omitted)

!
versión 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
interface GigabiteThernet0/0/0
 description Enlace a R2
 ip address 209.165.200.225 255.255.255.252
 negotiation auto
!
```

```
interface GigabitEthernet0/0/1
 description Enlace a LAN
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
!
router ospf 10
 network 192.168.10.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.3 area 0
!
banner motd ^C ¡Solamente acceso autorizado! ^C
!
líne con 0
 password 7 14141B180F0B
 login
line vty 0 4
 password 7 00071A150754
 login
```

```
 transport input telnet ssh
!
end
R1#
```

Comando **show interfaces:** Verifica el estado de la interfaz y muestra cualquier mensaje de error.

```
R1# show interfaces
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia
a0e0.af0d.e140)
  Description: Enlace a R2
  Internet address is 209.165.200.225/30
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:21, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  5127 packets input, 590285 bytes, 0 no buffer
  Received 29 broadcasts (0 IP multicasts)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 5043 multicast, 0 pause input
  0 watchdog, 5043 multicast, 0 pause input
  0 output errors, 0 collisions, 2 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  1 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out
```

Comando **show ip interface:** Verifica la información de la Capa 3 de una interfaz.

```
R1# show ip interface
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 209.165.200.225/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
```

```
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
IP Null turbo vector
Associated unicast routing topologies:
      Topology "base", operation state is UP
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
```

```
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
IPv4 WCCP Redirect outbound is disabled
IPv4 WCCP Redirect inbound is disabled
IPv4 WCCP Redirect exclude is disabled
```

Comando **show arp:** Verifica la lista de hosts conocidos en la LAN de Ethernet local.

```
R1# show arp
Protocol  Address          Age (min) Hardware Addr Type Interface
Internet  192.168.10.1       - a0e0.af0d.e141 ARPA GigabitEthernet0/0/1
Internet  192.168.10.10     95 c07b.bcc4.a9c0 ARPA GigabitEthernet0/0/1
Internet  209.165.200.225    - a0e0.af0d.e140 ARPA GigabitEthernet0/0/0
Internet  209.165.200.226   138 a03d.6fe1.9d90 ARPA
GigabitEthernet0/0/0
R1#
```

Comando **show ip route:** Verifica la información de enrutamiento de la Capa 3.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
   E1 - OSPF external type 1, E2 - OSPF external type 2
   i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
   ia - IS-IS inter area, * - candidate default, U - per-user static
route
   o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
   a - application route
   + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:50,
GigabitEthernet0/0/0
   10.0.0.0/24 is subnetted, 1 subnets
O    10.1.1.0 [110/3] via 209.165.200.226, 02:05:42, GigabitEthernet0/0/0
   192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
   209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C    209.165.200.224/30 is directly connected, GigabitEthernet0/0/0
L    209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
O    209.165.200.228/30 [110/2] via 209.165.200.226, 02:07:19,
GigabitEthernet0/0/0
R1#
```

Comando **show protocols:** Verifica cuáles protocolos están operativos

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 209.165.200.225/30
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
Serial0/1/0 is down, line protocol is down
Serial0/1/1 is down, line protocol is down
GigabitEthernet0 is administratively down, line protocol is down
R1#
```

Comando **show version:** Verifica la memoria, las interfaces y las licencias del dispositivo

```
R1# show version
Cisco IOS XE Software, Version 03.16.08.S - Extended Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 15.5(3)S8, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 08-Aug-18 10:48 by mcpre
```

```
ROM: IOS-XE ROMMON
R1 uptime is 2 hours, 25 minutes
Uptime for this control processor is 2 hours, 27 minutes
System returned to ROM by reload
System image file is "bootflash:/isr4300-universalk9.03.16.08.S.155-
3.S8-ext.SPA.bin"
Last reload reason: LocalSoft
```

```
Technology     Technology-package     Technology-package
               Current      Type          Next reboot
------------------------------------------------------------------
appxk9         appxk9       RightToUse    appxk9
uck9           None         None          None
securityk9     securityk9   Permanent     securityk9
ipbase         ipbasek9     Permanent     ipbasek9
cisco ISR4321/K9 (1RU) processor with 1647778K/6147K bytes of memory.
Processor board ID FLM2044W0LT
2 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
978928K bytes of USB flash at usb0:.
Configuration register is 0x2102
R1#
```

10.3.3 Packet Tracer - Uso de los Comandos Show del IOS de Cisco

Packet Tracer: Utilizar los comandos show de Cisco IOS

Objetivos: Utilizar los comandos **show** de Cisco IOS

Aspectos básicos/situación

Los comandos **show** de Cisco IOS se usan muy frecuentemente al trabajar con equipos Cisco. En esta actividad, usaremos los comandos **show** en un router ubicado en un ISP.

Instrucciones

Parte 1: Conectarse al router Cisco 4321 del ISP.

En esta parte, utilizará el software de emulación de terminal en la PC del ISP para conectarse al enrutador Cisco 4321.

a. Haga clic en **ISP PC**.
b. Haga clic en la ficha **Desktop** (Escritorio). Seleccione **Terminal**. Revise la configuración del terminal y haga clic en **OK** (Aceptar) para continuar.
c. La línea **ISPRouter >** indica que está en el modo EXEC de usuarios. Presione Enter (Intro) si la línea de comandos no aparece.

Parte 2: Aprender los comandos show.

Use la información que muestran los comandos **show** para responder las siguientes preguntas.

Paso 1: Explore los comandos show en el modo EXEC de usuario.

a. Escriba **show ?** en la línea de comandos.
Mencione algunos comandos **show** más que estén disponibles en el modo EXEC de usuario.

Rpta: *Estos son algunos de los comandos show disponibles: show cdp, show class-map, show clock.*

b. Introduzca **show arp** en el cursor. Registre la dirección MAC y la dirección IP.

Las respuestas pueden variar. 0001.96CD.2501: 209.165.201.1, 000A.F3C7.5CD3: 209.165.201.5, y 0002.162C.67A7: 209.165.201.10

c. Introduzca **show flash** en el cursor. Registre la imagen de IOS que se indica.

Rpta: *ISR4300-universalK9.03.16.05.S.155-3.s5-ext.spa.bin*

d. Escriba **show ip route** en la línea de comandos.

¿Cuántas rutas aparecen en la tabla? **Rpta:** *2*

e. Escriba **show interfaces** en la línea de comandos. ¿Qué interfaz se encuentra activa y en funcionamiento?

Interfaz	Estado	Protocolo
GigabitEthernet 0/0/0	Activo	Activo
GigabitEthernet 0/0/1	Administratively Down	Inactivo
Serial0/1/0	Inactivo	Inactivo
Serial0/1/1	Inactivo	Inactivo

f. Escriba **show ip interfaces** en la línea de comandos. Según la salida de **show ip interface** ¿qué interfaz está conectada? **GigabitEthernet0/0/0**

g. Escriba **show version** en la línea de comandos. ¿Qué paquete de tecnología está habilitado en este momento en el router? **ipbasek9 y securityk9**

h. Introduzca **show protocols** en el cursor. ¿Qué protocolos están habilitados actualmente en el enrutador? **Internet Protocol routing is enabled. Line protocol is up for GigabitEthernet0/0/0.**

i. Ingrese **show running-config** en el indicador. ¿Cuál es la salida?

ISPRouter> show running-config
^
% Invalid input detected at '^' marker.

Paso 2: Explorar los comandos show en el modo EXEC de usuario.

a. Introduzca **enable** en la línea de comandos para ingresar al modo EXEC con privilegios. Mencione algunos otros comandos **show** en este modo.

Rpta: *Algunos ejemplos de los comandos show son: show aaa, show access-list, show file*

b. Ingrese **show running-config** en el indicador. ¿Cuál es la salida?

Rpta: *La salida muestra las configuraciones y los ajustes actuales.*

4. Resumen de la línea de comandos del IOS de Cisco

10.4.1 ¿Qué Aprendí en este Módulo?

Navegación de IOS
La CLI del IOS de Cisco es un programa basado en texto que permite ingresar y ejecutar comandos del IOS de Cisco para configurar, monitorear y mantener los dispositivos de Cisco. La CLI de Cisco puede ser utilizada para tareas de administración tanto dentro de banda como fuera de banda.

Utilice los comandos de la CLI para modificar la configuración del dispositivo y para mostrar el estado actual de los procesos del enrutador. Cuando el enrutador ha completado la secuencia de encendido y aparece el indicador Router>, se puede utilizar la CLI para ingresar los comandos del IOS de Cisco.

Como característica de seguridad, el software IOS de Cisco divide el acceso de administración en los siguientes dos modos de comando:

- **Modo EXEC usuario** - Este modo resulta útil para operaciones básicas. Permite una cantidad limitada de comandos de monitoreo básicos, pero no permite la ejecución de ningún comando que podría cambiar la configuración del dispositivo. El modo EXEC del usuario se puede reconocer por la petición de entrada de la CLI que termina con el símbolo >.
- **Modo EXEC privilegiado**- Para ejecutar comandos de configuración, un administrador de redes debe acceder al modo EXEC privilegiado. El modo EXEC con privilegios se puede reconocer por la petición de entrada que termina con el símbolo #. Solo se puede ingresar al modo de configuración global y a los modos de configuración más altos por medio del modo EXEC con privilegios. El modo de configuración global se identifica mediante el indicador de CLI que termina en (config)#.

Los comandos utilizados para navegar entre los diferentes modos de comando de IOS son:

- enable
- disable
- configure terminal
- exit
- end
- Ctrl+Z
- line console 0
- line vty 0 15
- interface vlan 1

La estructura de comandos
Cada comando de IOS tiene una sintaxis o formato específico y puede ejecutarse solamente en el modo adecuado. La sintaxis general para un comando es el comando seguido de las palabras clave y los argumentos correspondientes. La palabra clave es un parámetro específico definido en el sistema operativo. El argumento no está predefinido; es un valor o variable definida por el usuario.

- La sintaxis proporciona el patrón o el formato que se debe utilizar cuando se introduce un comando. El **texto en negrita** indica los comandos y las palabras clave que se introducen literalmente como se muestran.
- El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.
- Los corchetes [x] indican un elemento opcional (palabra clave o argumento).
- Las llaves {x} indican un elemento obligatorio (palabra clave o argumento).

10.4.2 Webster - Preguntas de Reflexión

¿Alguna vez vio una película o un programa de televisión en el que una persona inteligente escribía en una computadora para evadir una medida de seguridad y obtener acceso no autorizado a los archivos? No estaban escribiendo una novela; estaban usando la interfaz de línea de comandos. Si bien puede emplear una interfaz de usuario para configurar la mayoría de los dispositivos de red, familiarizarse con los comandos y usarlos es mucho más rápido. Si debe solucionar los problemas de su red, deberá utilizar comandos. Sí, es como aprender un nuevo idioma, pero sabe de inmediato si lo hizo correctamente o no. Una vez que comienza a utilizar los comandos, es posible que nunca vuelva a la interfaz de usuario. ¿Qué le gustaría poder hacer con los comandos?

10.4.3 Prueba de La Línea de Comandos del IOS de Cisco

Haga coincidir la descripción con el modo IOS asociado.

Los cambios realizados afectan el funcionamiento del dispositivo como un todo	Modo de configuración global
Se accede ingresando el comando enable	Modo EXEC privilegiado
Identificado por un indicador que termina con el carácter #	Modo EXEC privilegiado
Número limitado de comandos básicos de monitoreo	Modo EXEC usuario
Se accede ingresando el comando configure terminal	Modo de configuración global
La primera entrada en la CLI de un dispositivo IOS	Modo EXEC usuario

¿Qué comando debe ejecutar un administrador para determinar qué interfaz utilizará un router para llegar a redes remotas?

show arp	show interfaces	show ip route ☺←	show protocols

Explique: El comando ***show ip route*** se utiliza para mostrar el contenido de la tabla de enrutamiento. La tabla de enrutamiento IP mostrará una lista de redes locales y remotas conocidas y las interfaces que utilizará el router para llegar a esas redes.

¿Qué comando proporcionará información sobre el estado de todas las interfaces, incluyendo el número de gigantes, runts y colisiones en la interfaz?

show running-config	show interfaces ☺←	show ip interface brief	show history

Explique: El comando ***show interfaces*** es el más completo en proporcionar información sobre interfaces. El comando ***show ip interface brief*** no proporciona información sobre gigantes, runts o colisiones. El comando ***show history*** proporciona un historial de los comandos que se utilizaron. El comando ***show running-config*** mostrará información de configuración, pero no información de estado.

¿Qué combinación de teclas de acceso rápido se utiliza para interrumpir un proceso de IOS?

Ctrl-Shift-X	Ctrl-Shift-6 ☺←	Ctrl-Z	Ctrl-C

¿Qué función tiene la tecla de tabulación al introducir un comando en IOS?

Anula el comando actual y vuelve al modo de configuración.	Sale del modo de configuración y vuelve al modo EXEC del usuario.
Desplaza el cursor hacia el principio de la línea siguiente.	Completa el resto de una palabra escrita parcialmente en un comando. ☺←

¿Cuál de los siguientes comandos o combinaciones de teclas le permite a un usuario regresar al nivel anterior en la jerarquía de comandos?

End	Exit ☺←	Ctrl-Z	Ctrl-C

Explique: El comando ***end*** y la combinación de teclas ***Ctrl-Z*** le permiten a un usuario regresar al modo EXEC privilegiado. ***Ctrl-C*** permite finalizar un comando en curso. El comando ***exit*** le permite al usuario regresar al nivel anterior.

Una las definiciones con los respectivos métodos abreviados y teclas de acceso rápido de la CLI.

cancela comandos como trace y ping	✓ Flecha Arriba
muestra la siguiente pantalla	✓ barra espaciadora
brinda ayuda sensible al contexto	✓ Tab
se desplaza hacia atrás a través de los comandos ingresados previamente	✓ ?
completa comandos y parámetros abreviados	✓ Ctrl-C

¿Cuáles son las dos afirmaciones verdaderas con respecto al modo EXEC del usuario? (Escoja dos.)

Todos los comandos del enrutador están disponibles.
Se puede acceder al modo de configuración global introduciendo el comando enable.
El indicador del dispositivo para este modo termina con el símbolo '>'. ☺←
Se pueden configurar interfaces y protocolos de enrutamiento.
Solo se pueden ver algunos aspectos de la configuración del enrutador. ☺←

Un administrador de red está trabajando en un router Cisco. El indicador de la CLI es Router1(config-if)#. ¿Cuál es la operación que probablemente configurará el administrador a continuación?

Las líneas vty	Una interfaz LAN ☺←
El puerto de consola	La contraseña que se necesita para acceder al modo EXEC con privilegios

Explicación: Cisco IOS utiliza distintos indicadores para identificar los modos de configuración específicos. El indicador ***Router1(config-if)#*** es un modo de subconfiguración de ***Router(config)#*** e indica que los comandos de configuración que siguen se aplican a interfaz LAN o WAN.

En el comando **show running-config**, ¿qué parte de la sintaxis está representada por **running-config**?

El comando	Una palabra clave ☺←	Una variable	Un indicador

Explique: La primera parte de la sintaxis, ***show***, es el comando, y la segunda parte de la sintaxis, ***running-config***, es la palabra clave. La palabra clave especifica lo que debe mostrarse como resultado del comando ***show***.

Un administrador de red emite el comando Switch(config)# **Interface FastEthernet 0/1** en un conmutador Cisco. ¿Qué término se utiliza para describir la parte **"0/1"** en el comando?

Teclas rápidas	Palabra clave	Argumento ☺←	Comando

Módulo 11: Crear una Pequeña Red de Cisco

0. Introducción

11.0.1 Webster - ¿Por Qué Debería Tomar este Módulo?

Hola, soy yo, Webster. Usted y Diego ahora tienen un buen conocimiento de las funciones de la línea de comandos del IOS de Cisco. Esto facilitará mucho la próxima tarea de Diego. En la nueva ubicación, deberá configurar y configurar todos los dispositivos, que incluirán dispositivos host, switches y routers, y todo el cableado necesario. Esta nueva red debe poder comunicarse con la red en la sede central, además de poder acceder a Internet. Esto es un poco más complicado que mi red doméstica, pero creo que podría hacerlo con un poco de ayuda. Por eso voy a tomar este módulo. ¡Espero que me acompañen!

11.0.2 ¿Qué Aprenderé en este Módulo?

- Título del módulo: Crear una Pequeña Red Cisco
- Objetivo del Módulo: Crear una red de computadoras simple con dispositivos Cisco.

Título del Tema	Objetivo del Tema
Configuración Básica del Conmutador	Configure los parámetros iniciales en un switch Cisco.
Configure los parámetros iniciales en un switch Cisco.	Configure los ajustes iniciales en un enrutador.
Asegurar los Dispositivos	Configure los dispositivos para la administración remota segura.
Configuración del gateway predeterminado	Configure dispositivos para utilizar el gateway predeterminado.

1. Configuración básica del Conmutador

11.1.1 Pasos Básicos en la Configuración de un Conmutador

El conmutador Cisco viene *preconfigurado* y solo necesita que se le asigne información de seguridad básica antes de conectarse a la red. Algunos elementos que suelen configurarse en el conmutador de una LAN son: *nombre de host, dirección IP de administración, contraseñas e información descriptiva.*

El nombre de host de un conmutador es el nombre configurado del dispositivo. Del mismo modo que a cada computadora o impresora se le asigna un nombre, los equipos de red se deben configurar con un nombre descriptivo. Se aconseja que el nombre del dispositivo incluya la ubicación donde se instalará el conmutador. Un ejemplo podría ser: SW_Bldg_R-Room_216.

Una dirección IP de administración solo es necesaria si tiene pensado configurar y administrar el conmutador a través de una conexión dentro de banda en la red. Una dirección de administración le permite llegar al dispositivo a través de *Telnet, SSH* o de *clientes HTTP*. La información de dirección IP que se debe configurar en un conmutador es esencialmente la misma que se configura en una PC: *dirección IP, máscara de subred y puerta de enlace predeterminada.*

Para proteger un conmutador LAN de Cisco, es necesario configurar contraseñas en cada uno de los diversos métodos de acceso a la línea de comandos. Los requisitos mínimos incluyen la asignación de contraseñas a los métodos de acceso remoto como Telnet, SSH y la conexión de consola. También debe asignar una contraseña al *modo privilegiado* en el que se realizan cambios de configuración.

Nota: Telnet envía el nombre de usuario y la contraseña como texto sin cifrar y no se considera seguro. SSH cifra el nombre de usuario y la contraseña y, por lo tanto, es un método más seguro.

Tareas de Configuración
Antes de configurar un conmutador, revise las siguientes tareas de configuración inicial del conmutador:

Configure el nombre del dispositivo.
- **hostname** *name*

Proteger el modo EXEC usuario.
- **line console 0**
- **password** *contraseña*
- **login**

Proteger el acceso remoto por Telnet y SSH.
- **line vty 0 15**
- **password** *contraseña*
- **login**

Proteja el modo EXEC con privilegios.
- **enable secret** *contraseña*

Proteja todas las contraseñas del archivo de configuración.
- **service password-encryption**

Proporcione una notificación legal.
- **banner motd** *delimitador mensaje delimitador*

Configurar la SVI (Switch Virtual Interface) de administración.
- **interface vlan 1**
- **ip address** *dirección-ip máscara-subred*
- **no shutdown**

Guarde la configuración.
- **copy running-config startup-config**

Ejemplo de configuración del Conmutador

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
S1(config)# banner motd #Prohibido el acceso no autorizado!#
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.1.20 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

11.1.2 Configuración de la Interfaz Virtual del Conmutador (SVI)

Para acceder al conmutador de manera remota, se deben configurar una dirección IP y una máscara de subred en la interfaz virtual del conmutador (SVI). Para configurar un SVI en un conmutador, use el comando de configuración global ***interface vlan 1***. La Vlan 1 no es una interfaz física real, sino una virtual. A continuación, asigne una dirección IPv4 mediante el comando de la configuración de interfaz ***ip address*** dirección-ip mascara -de-subred. Finalmente, habilite la interfaz virtual con el comando de configuración de interfaz ***no shutdown***.

Después de configurar el conmutador con estos comandos, el conmutador tiene todos los elementos IPv4 listos para la comunicación a través de la red local.

Nota: De manera similar a los hosts de Windows, los conmutadores configurados con una dirección IPv4 generalmente también deben tener una puerta de enlace predeterminada asignada. Esto se puede hacer mediante el comando de configuración global ***ip default-gateway*** *dirección-ip*. El parámetro *dirección-ip* sería la dirección IPv4 del enrutador local en la red, como se muestra en el ejemplo. Sin embargo, en este tema solo configurará una red con conmutadores y hosts. Los enrutadores se configurarán más adelante.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# interface vlan 1
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
Sw-Floor-1(config-if)# no shutdown
Sw-Floor-1(config-if)# exit
Sw-Floor-1(config)# ip default-gateway 192.168.1.1
```

11.1.3 Verificador de Sintaxis - Configuración de una Interfaz Virtual del Conmutador

Ingrese el modo de configuración de interfaz para la VLAN 1:
Switch(config)# interface vlan 1

Configure la dirección IPv4 como 192.168.1.20 y la máscara de subred como 255.255.255.0.:
Switch(config-if)# ip address 192.168.1.20 255.255.255.0

Habilitar la interfaz.:
Switch(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up

Ha configurado correctamente la interfaz virtual del switch para la VLAN 1.

11.1.4 Packet Tracer - Implementar la Conectividad Básica

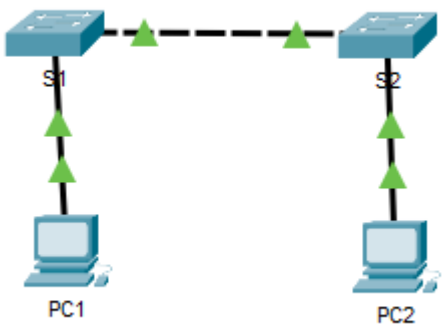
En esta actividad, cumplirá los siguientes objetivos:

- Realizar una configuración básica en el S1 y el S2
- Configurar las PCs
- Configurar la interfaz de administración de switches

Packet Tracer - Implementación de conectividad básica

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0



Objetivos

- **Parte 1:** Realizar una configuración básica de SVI en S1 y S2
- **Parte 2:** Configurar las PC

Aspectos básicos/Situación

En esta actividad, primero se efectuarán las configuraciones básicas del switch. Luego implementaremos la conectividad básica configurando las direcciones IP en los switches y PC. Cuando haya finalizado la configuración de la asignación de direcciones IP, utilizará diversos comandos **show** para verificar las configuraciones y utilizará el comando ping para verificar la conectividad básica entre los dispositivos.

Instrucciones

Parte 1: Realizar la configuración de SVI en S1 y S2

Paso 1: Configurar un nombre de host en el S1.

a. Haga clic en **S1** y, a continuación, haga clic en la ficha **CLI**.

b. Ingrese al modo EXEC con privilegios. Luego ingrese al modo de configuración global.

Switch> ***enable***
Switch# ***configure terminal***
Enter configuration commands, one per line. End with CNTL/Z.

c. Defina **S1** como nombre de host.

Switch(config)# ***hostname S1***
S1(config)#

Paso 2: Configurar S1 con una dirección IP.

Los switches se pueden usar sin ninguna configuración. Los switches reenvían información desde un puerto hacia otro sobre la base de direcciones de control de acceso al medio (MAC).

¿Por qué necesita un switch una dirección IP? ***Se requiere una dirección IP para conectarse a un switch de forma remota. El switch se administra mediante VLAN1 de manera predeterminada.***

a. En el modo de configuración global, introduzca los siguientes comandos para configurar S1 con una dirección IP en VLAN 1.

S1(config)# **interface vlan 1**
S1(config-if)# **ip address 192.168.1.253 255.255.255.0**
S1(config-if)# **no shutdown**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
¿Qué hace el comando **no shutdown**? ***El comando no shutdown habilita administrativamente el estado activo de la interfaz*.**

b. Salga del modo de configuración global y guarde la configuración.

S1(config-if)# ***end***
S1#
S1# ***copy running-config startup-config***
Destination filename [startup-config]?
Building configuration...
[OK]

c. Verificar la configuración de la dirección IP en S1.

S1# ***show ip interface brief***
<output omitted>
Vlan1 192.168.1.253 YES manual up

Paso 3: Configurar S2 con un nombre de host y una dirección IP.

En este paso, configurará S2 con un nombre de host y una dirección IP.

a. Haga click en **S2**. En la pestaña CLI, ingrese al modo de configuración global.

b. Configure el switch **S2** (conmutador) utilizando la información incluida en la tabla de direccionamiento.

c. Use la información en la tabla de direccionamiento, repita el mismo proceso para configurar el switch S2 con una dirección IP.

d. Salga del modo de configuración. Verificar la configuración de la dirección IP en S2.

*S2# **show ip interface brief***
<output omitted>
Vlan1 192.168.1.254 YES manual up

e. Guarde el archivo de configuración en la NVRAM. Escriba el comando **copy running-config startup-config** para guardar la configuración.

Parte 2: Configurar las PCs

En esta parte, configurará PC1 y PC2 con direcciones IP y verificará la conectividad de red.

Paso 1: Configure ambas PC con direcciones IP.

a. Haga clic en **PC1** y, luego haga clic en la pestaña **Desktop** (Escritorio).

b. Haga clic en **IP Configuration** (Configuración de IP). En la **Tabla de direcciones** anterior, puede ver que la dirección IP de PC1 debe ser 192.168.1.1 y la máscara de subred 255.255.255.0. Introduzca esta información para la PC1 en la ventana **Configuración de IP**.

c. Repita los pasos anteriores para PC2. Utilice la dirección IP que figura en la tabla de direcciones para PC2.

Paso 2: Pruebe la conectividad desde las PC.

a. Haga clic en **PC1**. Cierre la ventana **Configuración de IP** si todavía está abierta. En la ficha **Escritorio**, haga clic en **Símbolo del sistema**.

b. Ingrese el **comando** ping y la dirección IP de S1.

Packet Tracer PC Línea de comandos 1.0
*PC> **ping 192.168.1.253***
¿Tuvo éxito? Explique. **No, debería realizarse correctamente, porque los switches no están configurados con una dirección IP**.

f. Desde la PC1, haga ping a S2 y PC2.

g. Repita los pings a S1, S2 y PC1 desde PC2.

Todos los ping deben tener éxito. Si el resultado del primer ping es 80%, vuelva a intentarlo; ahora debería ser 100%. Más adelante, aprenderá por qué es posible que un ping falle la primera vez. Si no puede enviar un comando ping a ninguno de los dispositivos, revise la configuración en busca de errores.

Paso 3: Verifique la conectividad de la red desde los switches (conmutadores).
Puede verificarse la conectividad de la red mediante el comando **ping**. Es muy importante que haya conectividad en toda la red.

a. Desde S1, envíe un comando ping a los otros dispositivos en la red. A continuación, se muestra el ping a PC1 como ejemplo.

*S1> **ping 192.168.1.1***
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

b. Desde S2, envíe un comando ping a los otros dispositivos en la red.

Todos los ping deben tener éxito. Si el resultado del primer ping es 80%, vuelva a intentarlo; ahora debería ser 100%. Más adelante, aprenderá por qué es posible que un ping falle la primera vez. Si no puede enviar un comando ping a ninguno de los dispositivos, revise la configuración en busca de errores.

2. Configurar los ajustes iniciales del enrutador

11.2.1 Pasos Básicos de Configuración del Enrutador

Las siguientes tareas deben completarse al configurar inicialmente un enrutador.

Paso 1. Configure el nombre del dispositivo
Router(config)# **hostname** *nombredelhost*

Paso 2. Proteja el modo EXEC con privilegios
Router(config)# **enable secret** *password*

Paso 3. Proteger el modo EXEC de usuario
Router(config)# **line console 0**
Router(config-line)# **password** *contraseña*
Router(config-line)# **login**

Paso 4. Proteger el acceso remoto por Telnet y SSH.
Router(config-line)# **line vty 0 4**
Router(config-line)# **password** *contraseña*
Router(config-line)# **login**
Router(config-line)# **transport input {ssh | telnet | none | all}**

Paso 5. Proteja todas las contraseñas del archivo de configuración.
Router(config-line)# **exit**
Router(config)# **service password-encryption**

Paso 6. Proporcione una notificación legal.
Router(config)# **banner motd** *delimiter message delimiter*

Paso 7. Guarde la configuración.
Router(config)# **copy running-config startup-config**

11.2.2 Ejemplo de Configuración Básica del Enrutador

En este ejemplo, el enrutador R1 se configurará con la configuración inicial. Para configurar el nombre del dispositivo para R1, utilice los siguientes comandos.

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

Nota: Observe cómo el indicador del enrutador muestra ahora el nombre de host del enrutador.

Todo el acceso al enrutador debe estar asegurado. El modo EXEC privilegiado brinda al usuario acceso completo al dispositivo y su configuración, por lo que debe protegerlo.

Los siguientes comandos aseguran el modo EXEC privilegiado y el modo EXEC usuario, habilitan el acceso remoto Telnet y SSH y cifran todas las contraseñas de texto sin formato (es decir, EXEC de usuario y línea VTY). Es muy importante utilizar una contraseña segura al proteger el modo EXEC con privilegios, ya que este permite el acceso a la configuración del dispositivo.

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

La notificación legal advierte a los usuarios que solo deben acceder al dispositivo los usuarios permitidos. La notificación legal se configura de la siguiente manera:

```
R1(config)# banner motd #
Enter TEXT message. End with the character '#'.
**********************************************
WARNING: Unauthorized access is prohibited!
**********************************************
R1(config)#
```

Si el enrutador se configurara con los comandos anteriores y accidentalmente perdiera energía, la configuración del enrutador se perdería. Por esta razón, es importante guardar la configuración cuando se implementen los cambios. Los siguientes comandos guardan la configuración en ejecución en la NVRAM:

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

11.2.3 Verificador de Sintaxis - Configurar los Ajustes Iniciales del Enrutador

Utilice este comprobador de sintaxis para practicar la configuración inicial en un enrutador

- Configure el nombre del dispositivo.
- Proteger el modo EXEC con privilegios.
- Proteger y habilitar el acceso remoto por Telnet y SSH.
- Cifre todas las contraseñas de texto.
- Proporcione una notificación legal.

Ingrese al modo de configuración global para configurar el nombre del router como “R1”.

```
Router> enable
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# hostname R1
```

Configure “class” como contraseña secreta.

```
R1(config)# enable secret class
```

Configure “cisco” como contraseña de la línea de consola y solicite a los usuarios que inicien sesión.

```
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
```

Para vty línea 0 a 4, configure 'cisco' como la contraseña, requiera que los usuarios inicien sesión, habilite el acceso SSH y Telnet y regrese al modo de configuración global.

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
```

Cifre todas las contraseñas de texto no cifrado.

```
R1(config)# service password-encryption
```

Introduzca el aviso “¡Acceso autorizado únicamente!” y utilice ## como carácter delimitador.

```
R1(config)# banner motd #Authorized Access Only!#
```

Salga del modo de configuración global.

```
R1(config)# exit

R1#
```

Ha configurado correctamente la configuración inicial en el router R1.

11.2.4 Packet Tracer: Configurar los Parámetros Iniciales del Enrutador

Packet Tracer - Configuración inicial del enrutador

Objetivos

Parte 1: Verificar la configuración predeterminada del enrutador

Parte 2: Configurar y verificar la configuración inicial del enrutador

Parte 3: Guardar el archivo de configuración en ejecución

Aspectos básicos

En esta actividad, realizará tareas básicas de configuración del enrutador. Asegurará el acceso a la CLI y al puerto de la consola utilizando contraseñas encriptadas y de texto sin formato. También configurará mensajes para los usuarios que inician sesión en el enrutador. Estos avisos advierten a los usuarios no autorizados que el acceso está prohibido. Por último, verificará y guardará la configuración en ejecución.

Instrucciones

Parte 1: Verifique la configuración predeterminada del enrutador

Paso 1: Establezca una conexión de consola al R1.

a. Elija un cable de **consola** de las conexiones disponibles.

b. Haga clic en **PCA** y seleccione **RS 232**.

c. Haga clic en **R1** y seleccione **Console**.

d. Haga clic en **PCA** > ficha **Desktop** > **Terminal**.

e. Haga clic en **OK** y presione **Enter**. Ahora puede configurar **R1**.

Paso 2: Ingrese al modo con privilegios y examinar la configuración actual.

Puede acceder a todos los comandos del enrutador en el modo EXEC privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con contraseña para evitar el uso no autorizado.

a. Ingrese al modo EXEC privilegiado introduciendo el comando **enable**.

Router> ***enable***
Router#

Observe que la petición de entrada cambia en la configuración para reflejar el modo EXEC con privilegios.

b. Ingrese el comando **show running-config**.

Router# ***show running-config***
¿Cuál es el nombre de host del enrutador? **Router**

¿Cuántas interfaces Fast Ethernet tiene el enrutador? **Ninguna**

¿Cuántas interfaces Gigabit Ethernet tiene el enrutador? **Dos**

¿Cuántas interfaces seriales tiene el enrutador? **Dos**

¿Cuál es el rango de valores que se muestra para las líneas vty? **0-4**

c. Muestre el contenido actual de la NVRAM.

Router# **show startup-config**
startup-config is not present
¿Por qué el enrutador responde con el mensaje **startup-config is not present**?: **Muestra ese mensaje porque el archivo de configuración del switch no se guardó en la NVRAM. Actualmente solo se encuentra en la RAM.**

Parte 2: Configure y verifique la configuración inicial del enrutador

Para configurar los parámetros de un enrutador, quizá deba pasar por diversos modos de configuración. Observe cómo cambia la solicitud a medida que navega por los modos de configuración de IOS.

Paso 1: Configure los parámetros iniciales del R1.

Nota: Si tiene dificultades para recordar los comandos, consulte el contenido de este tema.

a. Configure **R1** como el nombre del enrutador (hostname).

b. Configure el mensaje de texto del día: **Unauthorized access is strictly prohibited.**

c. Encripte todas las contraseñas de texto no cifrado.

Utilice las siguientes contraseñas:

1) EXEC privilegiado, encriptado: **itsasecret**

2) Consola: **letmein**

Paso 2: Verifique los parámetros iniciales del R1.

a. Para verificar los parámetros iniciales, observe la configuración del R1.Qué comando utiliza?: **show running-config**

b. Salga de la sesión de consola actual hasta que vea el siguiente mensaje:

R1 con0 is now available
Press RETURN to get started.

c. Presione **ENTER**; debería ver el siguiente mensaje:

Unauthorized access is strictly prohibited.
User Access Verification
Password:

¿Por qué todos los enrutadores deben tener un mensaje del día (MOTD)? **Cada enrutador debe tener un mensaje para advertir a los usuarios no autorizados que el acceso está prohibido. Los mensajes MOTD también se pueden utilizar para enviar mensajes al personal de la red (como por ejemplo apagados inminentes del sistema o a quién contactar para acceder).**

Si no se le solicita una contraseña antes de llegar al indicador EXEC del usuario, ¿qué comando de línea de consola olvidó configurar?

R1(config-line)# login

d. Introduzca las contraseñas necesarias para regresar al modo EXEC con privilegios.

Si configura más contraseñas en el enrutador, ¿se muestran como texto no cifrado o en forma cifrada en el archivo de configuración? Explique. **El comando service password-encryption encriptará todas las contraseñas actuales y futuras.**

Parte 3: Guarde el archivo de configuración en ejecución

Paso 1: Guarde el archivo de configuración en la NVRAM.

a. Ha configurado la configuración inicial para **R1**. Ahora haga una copia de respaldo del archivo de configuración en ejecución en la NVRAM para garantizar que no se pierdan los cambios realizados si el sistema se reinicia o se apaga.

¿Qué comando introdujo para guardar la configuración en la NVRAM? **copy running-config startup-config**

¿Cuál es la versión más corta e inequívoca de este comando? **cop r st**

¿Qué comando muestra el contenido de la NVRAM? **show startup-configuration o show start**

b. Verifique que todos los parámetros configurados estén registrados. De lo contrario, analice el resultado y determine qué comandos no se ejecutaron o se ingresaron incorrectamente. También puede hacer clic en **Check Results** en la ventana de instrucción.

Paso 2: Opcional: Guarde el archivo de configuración de inicio en flash.

Si bien aprenderá más sobre cómo administrar el almacenamiento flash en un enrutador en capítulos posteriores, es posible que le interese saber que, como procedimiento de respaldo adicional, puede guardar su archivo de configuración de inicio en flash. De manera predeterminada, el enrutador seguirá cargando la configuración de inicio desde la NVRAM, pero si esta se daña, puede restablecer la configuración de inicio copiándola de la memoria flash.

Complete los siguientes pasos para guardar la configuración de inicio en la memoria flash.

a. Examine el contenido de la memoria flash mediante el comando **show flash**:

R1# **show flash**

¿Cuántos archivos hay almacenados actualmente en la memoria flash? **Tres**

¿Cuál de estos archivos cree que es la imagen de IOS? **ISR4300-universalK9.03.16.05.S.155-3.s5-ext.spa.bin**

¿Por qué cree que este archivo es la imagen de IOS? **Las respuestas pueden variar, pero hay dos pistas: la longitud del archivo en comparación con otros y la extensión .bin al final del nombre de archivo**.

b. Utilice los siguientes comandos para guardar el archivo de configuración de inicio en la memoria flash:

*R1# **copy startup-config flash***

Destination filename [startup-config]

El enrutador le solicita almacenar el archivo en flash utilizando el nombre entre paréntesis. Si la respuesta es afirmativa, presione **ENTER**; de lo contrario, escriba un nombre adecuado y presione la tecla **ENTER**.

c. Utilice el comando **show flash** para verificar que el archivo de configuración de inicio esté guardado en la memoria flash.

3. Asegurar los dispositivos

11.3.1 Recomendaciones para Contraseñas

Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Las pautas estándar que se deben seguir son las siguientes:

- Use una contraseña de al menos ocho caracteres, preferiblemente 10 o más caracteres. Una contraseña más larga es una contraseña más segura.
- Cree contraseñas complejas. Incluya una combinación de letras mayúsculas y minúsculas, números, símbolos y espacios, si están permitidos.
- Evite las contraseñas basadas en la repetición, las palabras comunes de diccionario, las secuencias de letras o números, los nombres de usuario, los nombres de parientes o mascotas, información biográfica (como fechas de nacimiento), números de identificación, nombres de antepasados u otra información fácilmente identificable.
- Escriba una contraseña con errores de ortografía a propósito. Por ejemplo, Smith = Smyth = 5mYth, o Seguridad = 5egur1dad.
- Cambie las contraseñas con frecuencia. Si una contraseña se ve comprometida sin saberlo, la ventana de oportunidad para que el actor de la amenaza use la contraseña es limitada.
- No anote las contraseñas ni las deje en lugares obvios, por ejemplo, en el escritorio o el monitor.

Las tablas muestran ejemplos de contraseñas seguras y débiles.

Contraseña débil	Porqué es débil
secreto	Contraseña de diccionario simple
Pérez	Nombre de soltera de la madre
Toyota	Marca de auto
Bob1967	Nombre y cumpleaños del usuario
Blueleaf23	Palabras y números simples

Contraseña segura	Porqué es segura
B67n423d9c	Combinación de caracteres alfanuméricos
12[h u4@1p7	Combina caracteres alfanuméricos, símbolos y un espacio

En los enrutadores Cisco, se ignoran los espacios iniciales para las contraseñas, pero no ocurre lo mismo con los espacios que le siguen al primer carácter. Por lo tanto, un método para crear una contraseña segura es utilizar la barra espaciadora y crear una frase compuesta de muchas palabras. Esto se conoce como frase de contraseña. Una frase de contraseña suele ser más fácil de recordar que una contraseña simple. Además, es más larga y más difícil de descifrar.

11.3.2 Acceso Remoto Seguro

Existen muchas maneras de obtener acceso a un dispositivo para ejecutar tareas de configuración. Una es utilizar una PC conectada al puerto consola del dispositivo. Este tipo de conexión se usa frecuentemente para la configuración inicial del dispositivo.

La configuración de una contraseña para el acceso a la conexión de consola se realiza en el modo de configuración global. Estos comandos evitan que los usuarios no autorizados accedan al modo usuario desde el puerto de consola.

```
Switch(config)# line console 0
Switch(config-line)# password password
Switch(config-line)# login
```

Cuando el dispositivo se conecta a la red, se puede acceder a él a través de la conexión de red mediante SSH o Telnet. SSH es el método preferido porque es más seguro. Cuando se accede al dispositivo a través de la red, se considera que es una conexión ***vty***. La contraseña debe asignarse al puerto ***vty***. La siguiente configuración se utiliza para habilitar el acceso SSH al conmutador.

```
Switch(config)# line vty 0 15
Switch(config-line)# password password
Switch(config-line)# transport input ssh
Switch(config-line)# login
```

Un ejemplo de configuración se muestra en la ventana de comandos.

```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)#
```

De manera predeterminada, muchos conmutadores Cisco admiten hasta 16 líneas vty que se numeran del 0 al 15. El número de líneas vty que admite un enrutador Cisco varía según el tipo de enrutador y la versión de IOS. No obstante, la cantidad más frecuente de líneas vty configuradas es 5 en un enrutador. Estas líneas se numeran del ***0 al 4*** de manera predeterminada, aunque se pueden configurar líneas adicionales. Es necesario establecer una contraseña para todas las líneas vty disponibles. Puede configurarse la misma contraseña para todas las conexiones.

Para verificar que las contraseñas estén configuradas correctamente, utilice el comando ***show running-config***. Estas contraseñas se guardan en la configuración en ejecución como texto sin cifrar. Es posible establecer la encriptación en todas las contraseñas guardadas en el enrutador de manera que no puedan ser leídas fácilmente por individuos no autorizados. El comando de configuración global ***service password-encryption*** garantiza que todas las contraseñas estén encriptadas.

Con el acceso remoto protegido en el conmutador, ahora puede configurar SSH.

11.3.3 Habilitar SSH

Antes de configurar SSH, el conmutador debe tener configurado, como mínimo, un nombre de host único y los parámetros correctos de conectividad de red.

Paso 1. Verificar la compatibilidad con SSH.

Use el comando **show ip ssh** para verificar que el conmutador admita SSH. Si el conmutador no ejecuta un IOS que admita características criptográficas, este comando no se reconoce.

Paso 2. Configurar el dominio IP.
Configure el nombre de dominio IP de la red mediante el comando de modo de configuración global ***ip domain-name*** *nombre-de-dominio*. En la siguiente configuración de ejemplo, el valor del *nombre de dominio* es **cisco.com**.

Paso 3. Generar pares de claves RSA.
No todas las versiones del IOS utilizan la versión 2 de SSH de manera predeterminada, y la versión 1 de SSH tiene fallas de seguridad conocidas. Para configurar la versión 2 de SSH, emita el comando ***ip ssh version 2*** en el modo de configuración global. La creación de un par de claves RSA habilita SSH automáticamente. Utilice el comando de modo de configuración global ***crypto key generate rsa*** para habilitar el servidor SSH en el conmutador y generar un par de claves RSA. Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo. La configuración de ejemplo en la figura 1 utiliza un tamaño de módulo de 1024 bits. Una longitud de módulo mayor es más segura, pero se tarda más en generarla y utilizarla.
Nota: para eliminar el par de claves RSA, use el comando ***crypto key zeroize rsa*** en el modo de configuración global. Después de eliminarse el par de claves RSA, el servidor SSH se deshabilita automáticamente.

Paso 4. Configurar la autenticación de usuario.
El servidor SSH puede autenticar a los usuarios localmente o usar un servidor de autenticación. Para usar el método de autenticación local, cree un par de nombre de usuario y contraseña con el comando ***username*** *nombre-de-usuario* ***secret*** *contraseña* en modo de configuración global. En el ejemplo, al usuario **admin** se le asignó la contraseña **ccna**.

Paso 5. Configurar las líneas vty.
Habilite el protocolo SSH en las líneas vty mediante el comando ***transport input ssh*** del modo de configuración de línea. El conmutador Catalyst 2960 tiene líneas vty que van de 0 a 15. Esta configuración evita las conexiones que no son SSH (como Telnet) y limita al conmutador a que acepte solo las conexiones SSH. Use el comando ***line vty*** del modo de configuración global y, luego, el comando ***login local*** del modo de configuración de línea para requerir la autenticación local de las conexiones SSH mediante la base de datos de nombres de usuarios locales.

Paso 6. Habilitar la versión 2 de SSH.
De manera predeterminada, SSH admite las versiones 1 y 2. Si se admiten ambas versiones, en el resultado de ***show ip ssh*** se muestra que está habilitada la versión 1.99. La versión 1 tiene vulnerabilidades conocidas. Por esta razón, se recomienda habilitar únicamente la versión 2. Habilite la versión de SSH mediante el comando de configuración global ***ip ssh version 2***.

```
S1# show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys (of at least 768 bits size) to enable SSH v2.
Authentication timeout: 120 secs; Authentication retries: 3
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
```

```
S1(config)# username admin secret ccna
S1(config-line)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)# exit
S1#
```

11.3.4 Verificador de Sintaxis - Configuración de SSH

Use el Verificador de Sintaxis para configurar SSH en el conmutador S1

Set the domain name to **cisco.com** and generate the **1024** bit rsa key.

```
S1(config)# ip domain-name cisco.com

S1(config)# crypto key generate rsa

The name for the keys will be: S1.cisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your General Purpose Keys. Choosing a key modulus g

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 4 seconds)
```

```
S1(config)#
*Mar 1 02:20:18.529: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Create a local user **admin** with the password **ccna**. Set all vty lines to use ssh and local login for remote connections. Exit out to global configuration mode.

```
S1(config)# username admin secret ccna

S1(config)# line vty 0 15

S1(config-line)# transport input ssh

S1(config-line)# login local

S1(config-line)# exit
```

```
S1(config)#
%SYS-5-CONFIG_I: Configured from console by console
```

Configure S1 to use SSH 2.0.

```
S1(config)# ip ssh version 2

S1(config)#
```

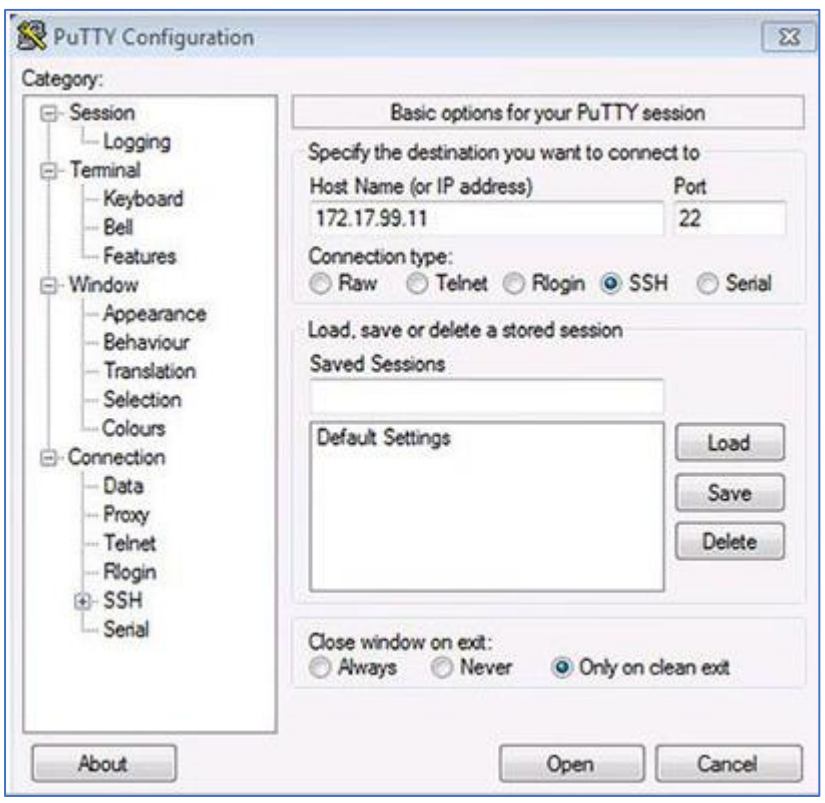
You successfully configured SSH on all VTY lines.

11.3.5 Verificar SSH

En las computadoras se usa un cliente SSH, como ***PuTTY***, para conectarse a un servidor SSH. Para los ejemplos se ha configurado lo siguiente:

- Se habilitó SSH en el conmutador S1
- Interfaz VLAN 99 (SVI) con la dirección IPv4 172.17.99.11 en el conmutador S1
- PC1 con la dirección IPv4 172.17.99.21

En la figura, el técnico está iniciando una conexión SSH a la dirección IPv4 de SVI VLAN de S1. Se muestra el software de terminal PuTTY.



Después de hacer clic en Abrir en PuTTY, se le solicita al usuario un nombre de usuario y una contraseña. Usando la configuración del ejemplo anterior, se ingresan el nombre de usuario **admin** y la contraseña **ccna**. Después de introducir la combinación correcta, el usuario se conecta a la CLI del switch Catalyst 2960 mediante SSH.

Para mostrar los datos de la versión y de configuración de SSH en el dispositivo que configuró como servidor SSH, use el comando ***show ip ssh***. En el ejemplo, se habilitó la versión 2 de SSH. Para verificar las conexiones SSH al dispositivo, use el comando ***show ssh***.

```
Login as: admin
Using keyboard-interactive authentication.
Password: <ccna>
```

```
S1> enable
Password: <class>
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAaP3fyrKmVi
PpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==
```

```
S1# show ssh
Connection Version Mode Encryption  Hmac        State         Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started admin
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started admin
%No SSHv1 server connections running.
S1#
```

11.3.6 Packet Tracer - Configurar SSH

En esta actividad, cumplirá los siguientes objetivos:

- Contraseñas seguras
- Cifrar las comunicaciones
- Verificar la implementación de SSH

Packet Tracer - Configure SSH

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objetivos

Parte 1: Proteger las contraseñas

Parte 2: Cifrar las comunicaciones

Parte 3: Verificar la implementación de SSH

Aspectos básicos/Situación

SSH debe reemplazar a Telnet para las conexiones de administración. Telnet usa comunicaciones inseguras de texto no cifrado. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro de todos los datos transmitidos entre los dispositivos. En esta actividad, protegerá un conmutador remoto con el cifrado de contraseñas y SSH.

Instrucciones

Parte 1: Contraseñas seguras

a. Desde el símbolo del sistema en la **PC1**, acceda a **S1** mediante Telnet. La contraseña de los modos EXEC de usuario y EXEC con privilegios es **cisco**.

```
PC> telnet 10.10.10.2
Trying 10.10.10.2 ...Open

User Access Verification

Password:
S1> en
Password:
S1#
```

b. Guarde la configuración actual, de manera que pueda revertir cualquier error que cometa reiniciando el **S1**.

```
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

c. Muestre la configuración actual y observe que las contraseñas están en texto no cifrado.

d. En el modo de configuración global, ingrese el comando que cifra las contraseñas de texto sin formato:

```
S1(config)# service password-encryption
```

e. Verifique que las contraseñas estén cifradas.

Parte 2: Cifrar las comunicaciones

Paso 1: Establecer el nombre de dominio IP y generar claves seguras.

En general no es seguro utilizar Telnet, porque los datos se transfieren como texto no cifrado. Por lo tanto, utilice SSH siempre que esté disponible.

a. Configure el nombre de dominio **netacad.pka.**

```
S1(config)# ip domain-name netacad.pka
```

b. Se necesitan claves seguras para cifrar los datos. Genere las claves RSA con la longitud de clave 1024.

```
S1(config)# crypto key generate rsa
The name for the keys will be: S1.netacad.pka
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Paso 2: Crear un usuario de SSH y reconfigurar las líneas VTY para que solo admitan acceso por SSH.

a. Cree un usuario **administrador** con **cisco** como contraseña secreta.

```
S1(config)# username administrator secret cisco
```

b. Configure las líneas VTY para que revisen la base de datos local de nombres de usuario en busca de las credenciales de inicio de sesión y para que solo permitan el acceso remoto mediante SSH. Elimine la contraseña existente de la línea vty.

```
S1(config)# line vty 0 15
S1(config-line)# login local
S1(config-line)# transport input ssh
S1(config-line)# no password cisco
```

Parte 3: Verificar la implementación de SSH

a. Cierre la sesión de Telnet e intente iniciar sesión nuevamente con Telnet. El intento debería fallar.

b. Intente iniciar sesión mediante SSH. Escriba **ssh** y presione la tecla **Enter**, sin incluir ningún parámetro que revele las instrucciones de uso de comandos. Sugerencia: la opción **-l** representa la letra “L”, no el número 1.

c. Cuando inicie sesión de forma correcta, ingrese al modo EXEC con privilegios y guarde la configuración. Si no pudo acceder de forma correcta al **S1**, reinicie y comience de nuevo en la parte 1.

```
----------------
Switch S1
----------------
enable
config terminal
service password-encryption
ip domain-name netacad.pka
crypto key generate rsa
1024
username administrator secret cisco
line vty 0 15
 login local
 transport input ssh
 no password cisco
end
```

4. Configuración de la puerta de enlace predeterminada

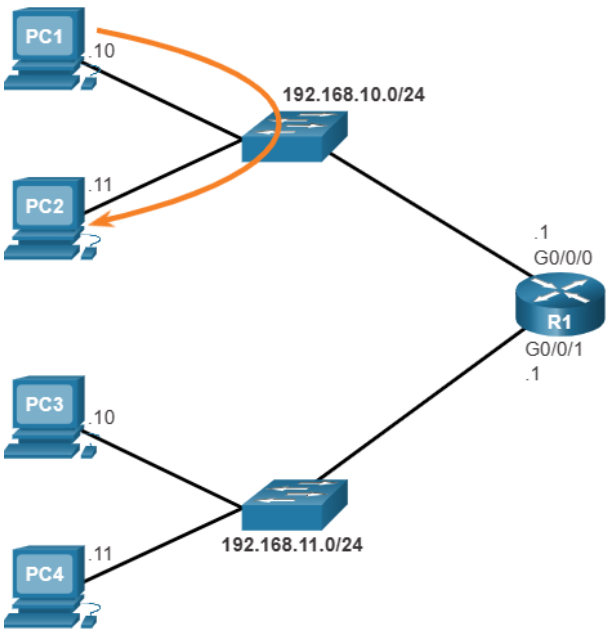
11.4.1 Puerta de Enlace Predeterminada en un Host

Si su red local sólo tiene un enrutador, será el enrutador de ***puerta de enlace*** y todos los hosts y conmutadores de su red deben estar configurados con esta información. Si la red local tiene varios enrutadores, debe seleccionar uno de ellos para que sea el enrutador de puerta de enlace predeterminado. En este tema se explica cómo configurar la puerta de enlace predeterminada en hosts y conmutadores.

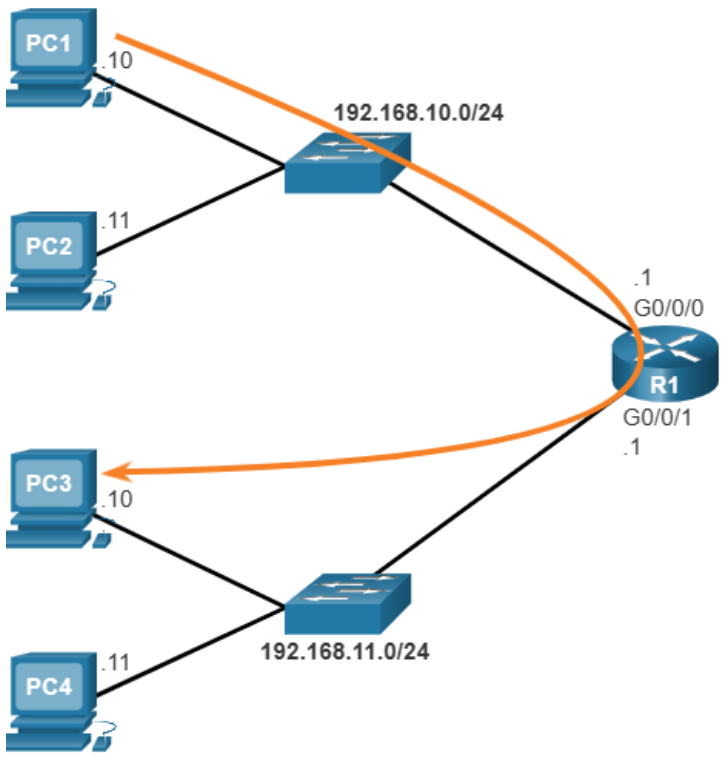
Para que un dispositivo final se comunique a través de la red, se debe configurar con la información de dirección IP correcta, incluida la dirección de la puerta de enlace predeterminada. La puerta de enlace predeterminada se usa solamente cuando el host desea enviar un paquete a un dispositivo de otra red. En general, la dirección de la puerta de enlace predeterminada es la dirección de la interfaz del enrutador conectada a la red local del host. La dirección IP del dispositivo host y la dirección de interfaz del enrutador deben estar en la misma red.

Por ejemplo, supongamos que una topología de red IPv4 consiste en un enrutador que interconecta dos LAN independientes. La interfaz ***G0/0*** está conectada a la red 192.168.10.0, mientras que la interfaz ***G0/1*** está conectada a la red 192.168.11.0. Cada dispositivo host está configurado con la dirección de la puerta de enlace predeterminada apropiada.

En este ejemplo, si PC1 envía un paquete a PC2, no utiliza la puerta de enlace predeterminada, sino que dirige el paquete con la dirección IPv4 de PC2 y lo reenvía directamente a PC2 a través del conmutador.



¿Qué pasa si PC1 envió un paquete a PC3? PC1 dirigirá el paquete con la dirección IPv4 de PC3, pero lo reenviará a su puerta de enlace predeterminada, que es la interfaz ***G0/0/0*** de R1. El enrutador acepta el paquete, accede a su tabla de enrutamiento para determinar la interfaz de salida apropiada según la dirección de destino. R1 reenvía el paquete por la interfaz apropiada para llegar a PC3.



El mismo proceso ocurriría en una red IPv6, aunque esto no se muestra en la topología. Los dispositivos usarían la dirección IPv6 del enrutador local como puerta de enlace predeterminada.

11.4.2 Puerta de Enlace Predeterminada en un Conmutador

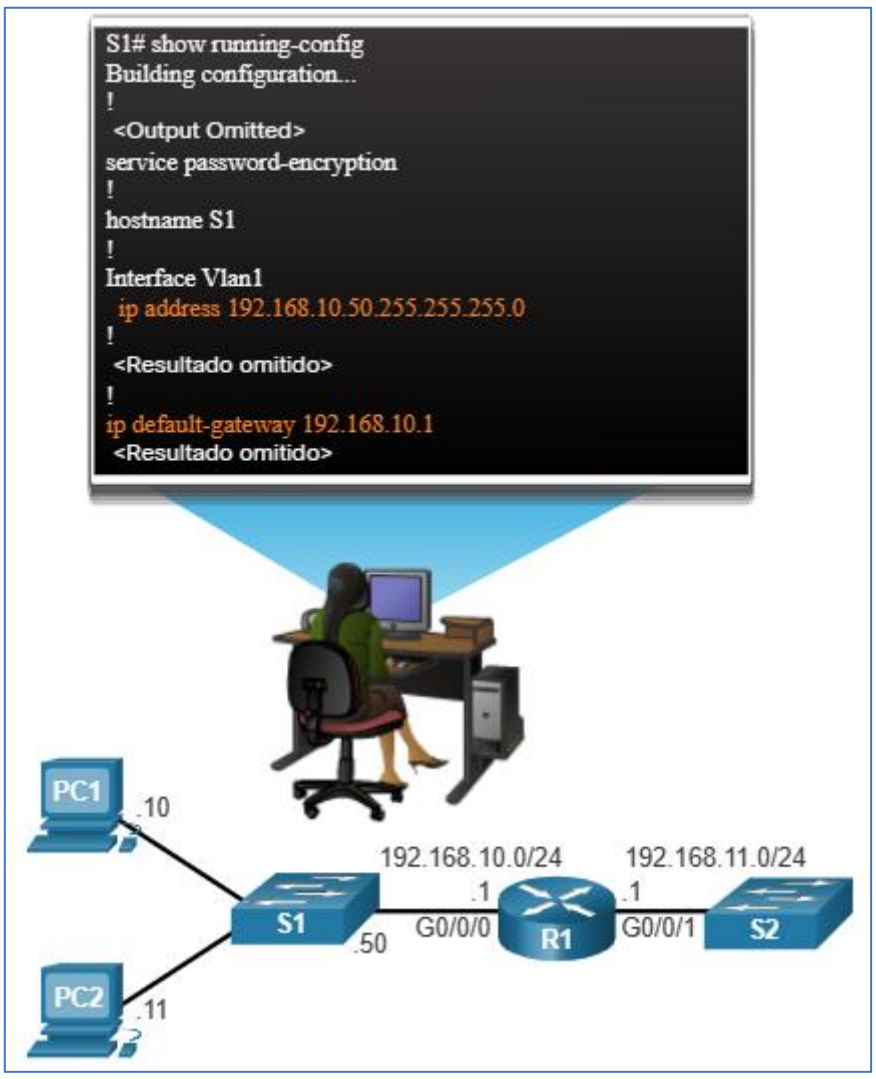
Un conmutador que interconecta equipos cliente suele ser un ***dispositivo de capa 2***. Como tal, un conmutador de capa 2 no requiere una dirección IP para funcionar correctamente. Sin embargo, se puede configurar una configuración IP en un conmutador para dar a un administrador acceso remoto al conmutador.

Para conectarse y administrar un conmutador a través de una red IP local, debe tener configurada una interfaz virtual de conmutador ***Switch Virtual Interface SVI***. El SVI se configura con una dirección IPv4 y una máscara de subred en la LAN local. El conmutador también debe tener una dirección de puerta de enlace predeterminada configurada para administrar el conmutador de forma remota desde otra red.

Por lo general, la dirección del gateway predeterminado se configura en todos los dispositivos que desean comunicarse más allá de la red local.

Para configurar una puerta de enlace predeterminada IPv4 en un conmutador, use el comando de configuración global ***ip default-gateway*** *dirección-ip*. La dirección IP que se configura es la dirección IPv4 de la interfaz del enrutador local conectada al conmutador.

En la figura se muestra un administrador que establece una conexión remota al conmutador S1 en otra red.

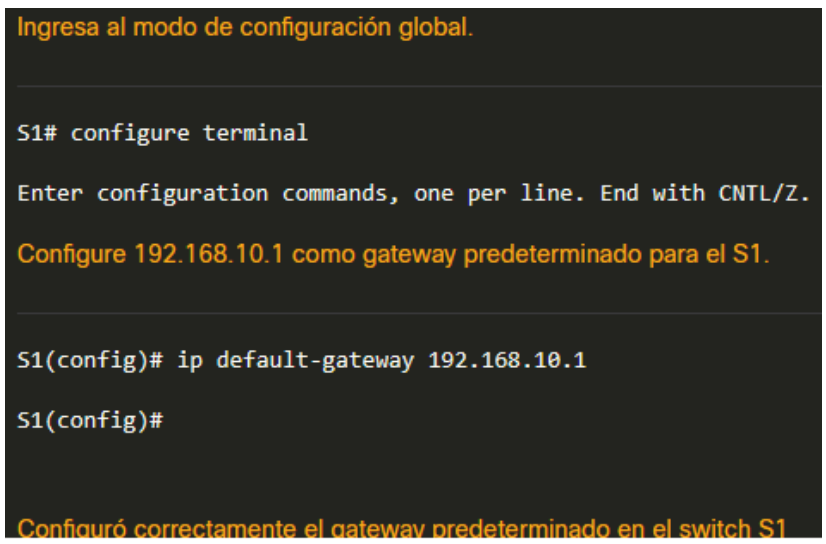


En este ejemplo, el host administrador usaría su puerta de enlace predeterminada para enviar el paquete a la interfaz ***G0/0/1*** de R1. R1 reenviaría el paquete a S1 desde su interfaz ***G0/0/0***. Dado que la dirección IPv4 de origen del paquete provenía de otra red, S1 requeriría una puerta de enlace predeterminada para reenviar el paquete a la interfaz ***G0/0/0*** de R1. Por lo tanto, el conmutador S1 se debe configurar con una puerta de enlace predeterminada, para que pueda responder y establecer una conexión SSH con el host administrativo.

Nota: Los paquetes que se originan en servidores conectados al conmutador ya deben crearse con la dirección de la puerta de enlace predeterminada configurada en el sistema operativo de su servidor.

Un conmutador de ***grupo de trabajo*** también se puede configurar con una dirección IPv6 en un SVI. Sin embargo, el conmutador no requiere que la dirección IPv6 de la puerta de enlace predeterminada se configure manualmente. El conmutador recibirá automáticamente su puerta de enlace predeterminada del mensaje ***ICMPv6 Router Advertisement*** del enrutador.

11.4.3 Verificador de Sintaxis — Configurar la Puerta de Enlace Predeterminada



11.4.4 Actividad Guiada de Packet Tracer - Crear una Red con un Conmutador y un Enrutador

Esta Actividad Guiada de Packet Tracer incluye un sistema de sugerencias y un tutorial incorporado. Conectará los dispositivos, configurará las PC, el enrutador, el conmutador y verificará la conectividad de punta a punta.

Objetivos

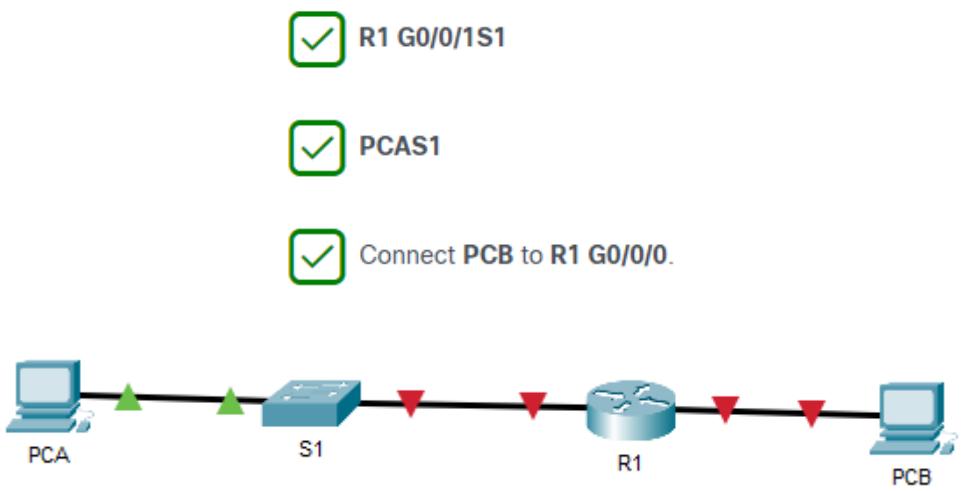
- Configurar las computadoras.
- Configure a router.
- Verifique la conectividad de extremo a extremo
- Configure a switch.
- Secure remote access to the router.

Trasfondo/Situación

Su tía es propietaria de una pequeña agencia de seguros. Recientemente adquirió un router y switch de Cisco. Tiene dos PC cableadas que deben conectarse a la red. Está orgullosa de su progreso en su curso de redes y le preguntó si le gustaría demostrar sus habilidades. Su trabajo es conectar los dispositivos, implementar una configuración básica y verificar la conectividad. Una vez verificada la conectividad de red, utilizará comandos IOS para recuperar información de los dispositivos para responder preguntas sobre su equipo de red. También configurará el router para un acceso remoto seguro.

Cuando esté listo, haga clic en **Siguiente** para empezar.

En primer lugar, conectará los dispositivos mediante cables directos de cobre. Conéctese a cualquier puerto activado.



Ha conectado correctamente todos los dispositivos de la red. Ahora es el momento de configurarlos. Haga clic en el botón **Siguiente** para continuar.

En este paso, asignará información de direccionamiento IPv4 estático a las interfaces de PC. Utilice la información de la tabla de direccionamiento para completar la tarea.

Dispositivo	Interfaz	Dirección IP	Mascara de subred	Puerta de enlace predeterminada
R1	G0/0/0	192.168.0.1	255.255.255.0	No corresponde
	G0/0/1	192.168.1.1	255.255.255.0	No corresponde
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PCA	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PCB	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Configurar la dirección IPv4, la máscara de subred y la puerta de enlace predeterminada en **PCA.**

- IP Address: **192.168.1.3**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.1.1**

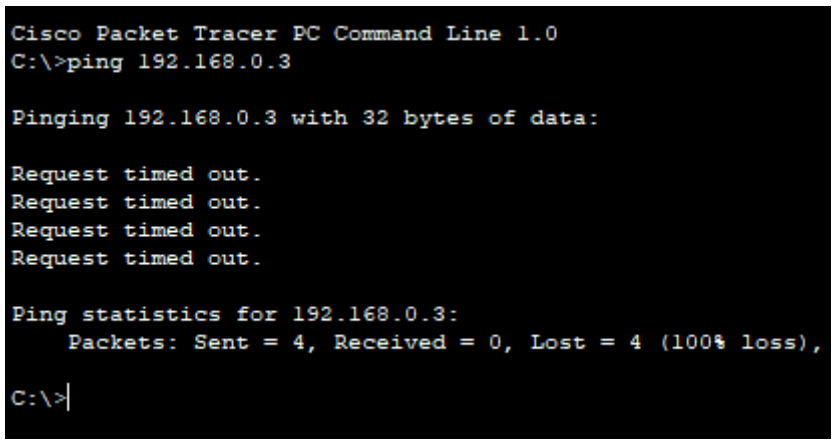
Configurar la dirección IPv4, la máscara de subred y la puerta de enlace predeterminada en **PCB.**

- IP Address: **192.168.0.3**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.0.1**

Ha configurado correctamente el direccionamiento IPv4 para las PC. Ahora debe verificar la conectividad entre ellos. Haga clic en el botón **Siguiente** para continuar.

Probar la conectividad entre PCA y PCB**. Haga ping entre PCA y PCB.**

- En el símbolo del sistema PCA, escriba el comando **ping 192.168.0.3**.
- También puede abrir el símbolo del sistema PCB y luego introducir el comando **ping 192.168.1.3**



Parece que el ping falló entre **PCA** y **PCB.** Click **Next** to continue.

¿Por qué los pings no tuvieron éxito? **Porque las luces de enlace en las conexiones del router son de color rojo. Esto indica que los enlaces no están funcionando.** Click **Next** to continue.

En este paso, utilizará la ficha CLI para configurar los ajustes básicos. Puede conectar un cable de consola en R1 y acceder a la CLI desde PCA o PCB si lo desea. Sin embargo, en esta actividad debe hacer clic en R1 para abrirla.

Asigne un nombre de host de acuerdo con la **tabla de direcciones**. Haga clic en **R1** Luego, introduzca el comando: Asignar una contraseña cifrada de EXEC con privilegios.

```
Router>enable
Router# configure terminal
Router(config)# hostname R1
```

class

```
R1(config)# enable secret class
```

cisco

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config)# service password-encryption
R1(config)# banner motd $Authorized Access Only!$
```

Para G0/0/0, configure el direccionamiento IP de acuerdo con la tabla de direccionamiento y active la interfaz.

```
R1(config)# interface g0/0/0
```

G0/0/0

```
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config)# no shutdown
```

G0/0/1

```
R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config)# exit
R1# copy running-config startup-config
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd $Authorized Access Only!$
R1(config)#interface g0/0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

R1(config-if)#interface g0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
R1(config)# exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Ha realizado correctamente la configuración básica requerida para **R1.** Click **Next** to continue. Ahora, vamos a probar la conectividad entre **PCA PCB** otra vez. Ping entre **PCA** y **PCB**. En el símbolo del sistema PCA, escriba el comando **ping 192.168.0.3.** También puede abrir el símbolo del sistema de PCB y luego ingresar el comando **ping 192.168.1.3.**

```
C:\> ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.3: bytes=32 time=1ms TTL=127
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Parece que funciona. Haga clic en el botón **Siguiente** para continuar.

¿Por qué fueron exitosos los pings entre PCA y PCB?
El router está enrutando el tráfico de ping a través de las dos redes. La configuración predeterminada para el conmutador 2960 habilita automáticamente las interfaces que están conectadas a los dispositivos.

Great. Click **Next** to continue. En este paso, usará la pestaña **CLI** para **S1** para configurar los ajustes básicos. Puede conectar un cable de consola y acceder a la CLI desde **PCA** o **PCB** si lo desea. Sin embargo, en esta actividad, puede hacer clic en **S1** para abrirlo. Asigne un nombre de host de acuerdo con la **tabla de direcciones**. Haga clic en **S1**. A continuación, introduzca el siguiente comando:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
```

Asigne **class** como contraseña cifrada EXEC privilegiada. Configure la contraseña del modo EXEC privilegiado en el modo de configuración global con el siguiente comando:

```
S1(config)# enable secret class
```

Asigne c**isco** como contraseña de la consola y habilite el inicio de sesión.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
```

Cifre contraseñas de texto sin formato con el siguiente comando en modo de configuración global:

```
S1(config)# service password-encryption
```

Cree un banner que advierta a cualquier persona que acceda al dispositivo que el acceso no autorizado está prohibido.

Configure un banner con el siguiente comando:

```
S1(config)# banner motd $Authorized Access Only!$
```

Para VLAN 1, configure el direccionamiento IP de acuerdo con la tabla de direccionamiento y active la interfaz.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
```

```
S1(config)# ip default-gateway 192.168.1.1
```

Guarde la configuración con el siguiente comando:

```
S1(config)# exit
S1# copy running-config startup-config
```

También puede utilizar el comando abreviado **copy run start** o el comando **write mem.**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# service password-encryption
S1(config)# banner motd $Authorized Acces Only!$
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)# ip default-gateway 192.168.1.1
S1(config)# exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Ha configurado correctamente **S1** con la configuración básica necesaria. Haga clic en **Siguiente** para continuar.

Acceso remoto seguro a **R1 activado. Configure el nombre de dominio como**: **R1academy.net R1ciscoclass**

Debe estar en modo de configuración global antes de continuar. Escriba el siguiente comando:

```
R1(config)# ip domain-name academy.net
```

Genere claves RSA con una longitud de clave **1024**.

```
R1(config)# crypto key generate rsa
```

Cree un usuario con **SSHuser** como nombre de usuario y c**isco** como contraseña secreta. Escriba el siguiente comando:

```
R1(config)# username SSHuser secret cisco
```

Configure las líneas VTY para usar la base de datos de nombres de usuario local para las credenciales de inicio de sesión. Las líneas VTY solo deben permitir SSH para el acceso remoto. Escriba el siguiente comando:

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
```

Ha configurado correctamente el acceso remoto seguro para **R1.** Click **Next** to continue. Ahora, verifiquemos el acceso remoto a SSH. Desde PCA o PCB, utilice el símbolo del sistema para establecer una sesión segura con R1. En el indicador, utilice el comando **ssh**

```
C:\> ssh -l SSHuser 192.168.1.1
```

```
C:\> ssh -l SSHuser 192.168.1.1

Password:

Authorized Access Only!

R1>
```

Ha verificado correctamente que SSH está configurado correctamente en **R1.** Haga clic en el botón **Siguiente** para continuar.

Si el estado de la interfaz G0/0/1 está administrativamente inactivo, ¿qué comando de configuración de interfaz usaría para activar la interfaz?

```
R1(config-if)# no shutdown
```

¿Qué pasaría si hubiera configurado incorrectamente la interfaz G0/0/1 en el router con una dirección IP de 192.168.1.2?

PC-A no podría hacer ping a PC-B. Esto se debe a que PC-B está en una red diferente a la PC-A. Se requiere el enrutador de puerta de enlace predeterminada para enrutar estos paquetes. PC-A está configurado para usar la dirección IP de 192.168.1.1 para el enrutador de puerta de enlace predeterminada, pero esta dirección no está asignada a ningún dispositivo en la LAN. Cualquier paquete que deba enviarse a la puerta de enlace predeterminada para el enrutamiento nunca llegará a su destino.

¡Felicitaciones! Ha conectado correctamente los dispositivos, ha implementado configuraciones básicas para PC, un router y un switch, y luego ha asegurado y verificado el acceso remoto al router.

11.4.5 Packet Tracer - Solución de Problemas de la Puerta de Enlace Predeterminada

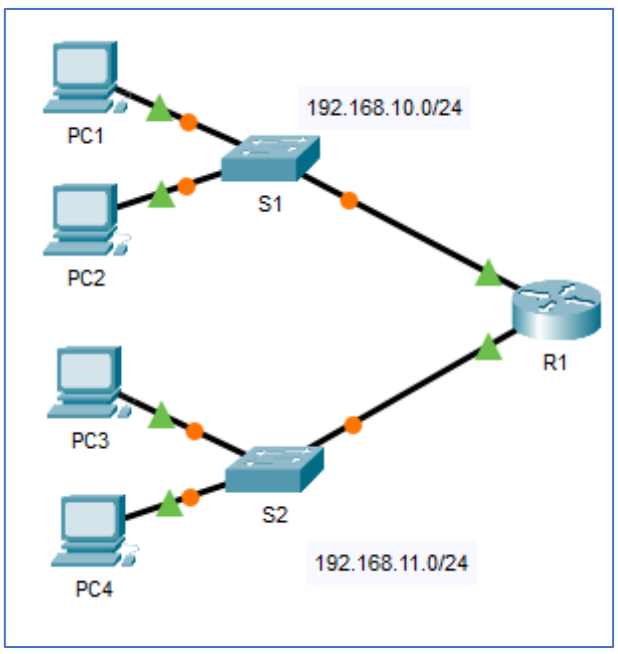
En esta actividad, cumplirá los siguientes objetivos:

- Verificar el registro de la red y descartar problemas
- Implemente, verifique y registre las soluciones

Packet Tracer - Solución de problemas del gateway predeterminado

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de enlace predeterminada
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
S1	VLAN 1	192.168.10.2	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.11.2	255.255.255.0	192.168.10.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC3	NIC	192.168.11.10	255.255.255.0	192.168.10.1
PC4	NIC	192.168.11.11	255.255.255.0	192.168.11.1



Objetivos

Parte 1: Verificar el registro de la red y descartar problemas

Parte 2: Implementar, verificar y registrar las soluciones

Aspectos básicos

Para que un dispositivo se comunique en varias redes, debe estar configurado con una dirección IP, una máscara de subred y un gateway predeterminado. La puerta de enlace predeterminada se usa cuando el host desea enviar un paquete a un dispositivo de otra red. La dirección de puerta de enlace predeterminada es generalmente la dirección de la interfaz del enrutador que está conectada a la red local a la que está conectado el host. En esta actividad, terminará de registrar la red. Luego, verificará el registro de la red mediante la prueba de la conectividad completa y la solución de problemas. Los métodos de solución de problemas que usted usará constan de los siguientes pasos:

a. Verifique el registro de la red y usar pruebas para aislar problemas.

b. Determine una solución apropiada para un problema determinado.

c. Implemente la solución.

d. Realice pruebas para verificar que se haya solucionado el problema.

e. Registre la solución.

A lo largo de sus estudios de CCNA, encontrará distintas descripciones del método de solución de problemas, así como distintas formas de probar y registrar problemas y soluciones. Esto es intencional. No existe un estándar o una plantilla establecida para la solución de problemas. Cada organización desarrolla procesos y estándares de registro exclusivos (incluso si ese proceso consiste en no tener ninguno). Sin embargo, todas las metodologías de resolución de problemas efectivas generalmente incluyen los pasos anteriores.

Nota: Si es competente con las configuraciones de puerta de enlace predeterminadas, esta actividad puede parecer más complicada de lo que debería ser. Lo más probable es que pueda descubrir y solucionar todos los problemas de conectividad más rápido que si siguiera estos procedimientos. No obstante, a medida que avance con sus estudios, las redes y los problemas que encuentre serán cada vez más complejos. En tales situaciones, la única forma eficaz de descartar y solucionar problemas es aplicar un enfoque metódico como el que se usa en esta actividad.

Instrucciones

Parte 1: Verificar el registro de la red y descartar problemas

En la parte 1 de esta actividad, completará el registro y realizará pruebas de conectividad para detectar problemas. Además, determinará la solución adecuada y la implementará en la parte 2.

Paso 1: Verifique el registro de la red y descartar cualquier problema.

a. Para que pueda probar una red con eficacia, debe contar con el registro completo. Observe que falta determinada información en la **tabla de direccionamiento**. Complete la **tabla de direccionamiento** con la información de gateway predeterminado que falta para los switches y las PC.

b. Pruebe la conectividad a los dispositivos en la misma red. Al descartar y corregir cualquier problema de acceso local, puede probar mejor la conectividad remota, con la seguridad de que la conectividad local funciona.

Un plan de verificación puede ser tan simple como una lista de pruebas de conectividad. Use las siguientes pruebas para verificar la conectividad local y descartar cualquier problema de acceso. El primer problema ya se registró, pero debe implementar y verificar la solución durante la parte 2.

Registro de prueba y verificación

Prueba	¿Se realizó correctamente?	Problemas	Solución	Verificado
PC1 a PC2	No	Dirección IP en la PC1	Cambiar la dirección IP de la PC1	
PC1 a S1				
PC1 a R1				

Nota: La tabla es un ejemplo; debes crear tu propio documento. Puede usar lápiz y papel para dibujar una tabla, o puede utilizar un editor de texto o una hoja de cálculo. Consulte al instructor si necesita más orientación.

c. Pruebe la conectividad a los dispositivos remotos (p. ej., de la PC1 a la PC4) y registre cualquier problema. Esto se conoce frecuentemente como "*conectividad completa*". Esto significa que la política de red permite que todos los todos los dispositivos en una red tengan conectividad plena.

Nota: La prueba de conectividad remota puede no ser posible todavía, porque primero debe resolver los problemas de conectividad local. Una vez que solucione dichos problemas, vuelva a este paso y pruebe la conectividad entre redes.

Paso 2: Determine cuál es la solución adecuada para el problema.

a. Con sus conocimientos sobre la forma en que operan las redes y sus aptitudes para configurar dispositivos, busque la causa del problema. Por ejemplo, el S1 no es la causa del problema de conectividad entre la PC1 y la PC2. Las luces de enlace son de color verde, y ninguna configuración en el S1 provocaría que no pase el tráfico entre la PC1 y la PC2. Por lo tanto, el problema debe de estar en la PC1, en la PC2 o en ambas.

b. Verifique el direccionamiento del dispositivo para asegurarse de que coincida con el registro de la red. Por ejemplo, la dirección IP para la PC1 es incorrecta, como se verificó con el comando **ipconfig**.

c. Sugiera una solución con la que usted crea que se solucionará el problema y regístrela. Por ejemplo, cambiar la dirección IP de la PC1 para que coincida con el registro.

Nota: A menudo hay más de una solución. Sin embargo, es una práctica recomendada para la resolución de problemas implementar y verificar una solución a la vez. Implemente más de una solución podría presentar problemas adicionales en una situación más compleja.

Parte 2: Implemente, verifique y registre las soluciones

En la parte 2 de esta actividad, implementará las soluciones que identificó en la parte 1. Luego, verificará si la solución funcionó. Es posible que deba volver a la parte 1 para terminar de descartar todos los problemas.

Paso 1: Implemente soluciones para abordar los problemas de conectividad.

Consulte el registro en la parte 1. Elija el primer problema e implemente la solución que sugirió. Por ejemplo, corrija la dirección IP en la PC1.

Paso 2: Verifique si ahora el problema está resuelto.

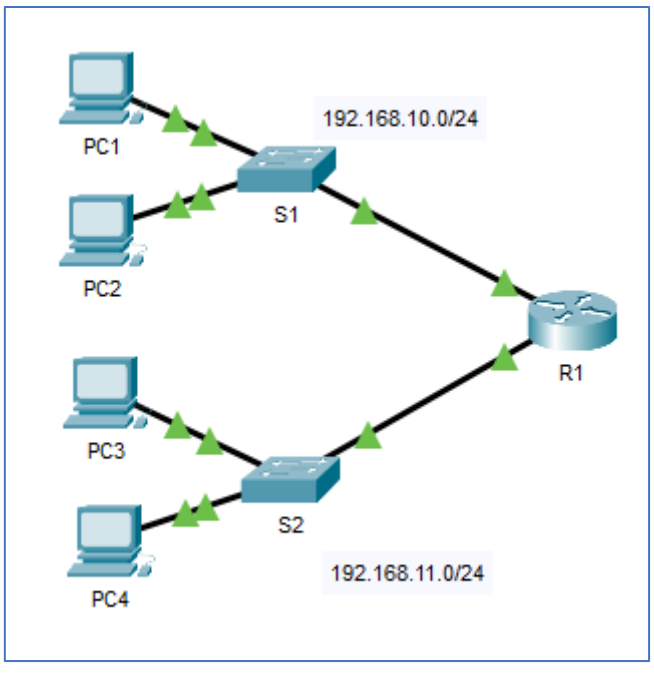
a. Verifique si la solución que propuso solucionó el problema realizando la prueba que usó para identificarlo. Por ejemplo, ¿la PC1 puede ahora hacer ping a la PC2?

b. Si el problema se solucionó, indíquelo en el registro. Por ejemplo, en la tabla anterior, con colocar una simple marca de verificación en la columna “Verificado” sería suficiente.

Paso 3: Verifique si se resolvieron todos los problemas.

a. Si todavía tiene un problema pendiente con una solución que aún no se implementó, vuelva al paso 1 de la parte 2.

b. Si se solucionaron todos los problemas actuales, ¿también solucionó todos los problemas de conectividad remota (por ejemplo, que la PC1 pueda hacer ping a la PC4)? Si la respuesta es negativa, vuelva al paso 1c de la parte 1 para probar la conectividad remota.



5. Resumen de crear una pequeña red de Cisco

11.5.1 ¿Qué Aprendí en este Módulo?

Configuración básica del Conmutador

Los elementos para configurar en un conmutador LAN incluyen el nombre del host, la información de la dirección IP de administración, las contraseñas y la información descriptiva. Una dirección de administración le permite llegar al dispositivo a través de Telnet, SSH o de clientes HTTP. La información de la dirección IP que debe configurarse en un conmutador incluye la dirección IP, la máscara de subred y la puerta de enlace predeterminada. Para proteger un conmutador LAN de Cisco, configure contraseñas en cada uno de los diversos métodos de acceso a la línea de comandos. Asigne contraseñas a métodos de acceso remoto, como Telnet, SSH y la conexión de la consola. También asigne una contraseña al modo privilegiado en el que se pueden realizar cambios de configuración.

Para acceder al conmutador de forma remota, configure una dirección IP y una máscara de subred en el SVI. Utilice el comando de configuración **global interface vlan 1**. Asigne una dirección IPv4 mediante el comando de la configuración de interfaz **ip address *dirección-ip mascara-de-subred*.** Finalmente, habilite la interfaz virtual con el comando de configuración de interfaz **no shutdown**. Después de configurar el conmutador con estos comandos, el conmutador tiene todos los elementos IPv4 listos para la comunicación a través de la red.

Configurar los ajustes iniciales del Router

Paso 1. Configure el nombre del dispositivo.
Paso 2. Proteja el modo EXEC con privilegios.
Paso 3. Proteger el modo EXEC de usuario.
Paso 4. Proteja el acceso remoto por Telnet/SSH.
Paso 5. Proteja todas las contraseñas del archivo de configuración.
Paso 6. Proporcione una notificación legal.
Paso 7. Guarde la configuración.

Todo el acceso al enrutador debe estar asegurado. El modo EXEC privilegiado brinda al usuario acceso completo al dispositivo y su configuración, por lo que debe protegerlo. Es muy importante utilizar una contraseña segura al proteger el modo EXEC con privilegios, ya que este permite el acceso a la configuración del dispositivo. La notificación legal advierte a los usuarios que solo deben acceder al dispositivo los usuarios permitidos. La configuración del enrutador se perdería si el enrutador pierde energía. Por esta razón, es importante guardar la configuración cuando se implementen los cambios.

Asegurar los dispositivos

Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Una contraseña segura combina caracteres alfanuméricos y, si está permitido, incluye símbolos y un espacio. Otro método para crear una contraseña segura es usar la barra espaciadora y crear una frase compuesta por muchas palabras, llamada frase de contraseña. Una frase de contraseña suele ser más fácil de recordar que una contraseña segura. Además, es más larga y más difícil de descifrar.

La configuración de una contraseña para el acceso a la conexión de consola se realiza en el modo de configuración global. Esto evita que los usuarios no autorizados accedan al modo de usuario desde el puerto de la consola. Cuando el dispositivo se conecta a la red, se puede acceder a él a través de la conexión de red mediante SSH o Telnet. SSH es el método preferido porque es más seguro. Cuando se accede al dispositivo a través de la red, se considera que es una conexión de vty. La contraseña debe asignarse al puerto vty. Cinco es el número más común de líneas vty configuradas en un enrutador. Estas líneas se numeran del 0 al 4 de manera predeterminada, aunque se pueden configurar líneas adicionales. Es necesario establecer una contraseña para todas las líneas vty disponibles. Puede configurarse la misma contraseña para todas las conexiones.

Para verificar que las contraseñas estén configuradas correctamente, utilice el comando **show running-config**. Estas contraseñas se guardan en la configuración en ejecución como texto sin cifrar. Es posible establecer cifrado en todas las contraseñas almacenadas en el enrutador. El comando de configuración global **service password-encryption** garantiza que todas las contraseñas estén encriptadas.

Habilitación de SSH

Paso 1. Verificar la compatibilidad con SSH - **show ip ssh**
Paso 2. Configure el dominio IP - **ip domain-name** *nombre-de-dominio*
Paso 3. Generar pares de claves RSA - **crypto key generate rsa**
Paso 4. Configure la autenticación de usuario - **username** *nombre-de-usuario* **secret** *contraseña*
Paso 5. Configure las líneas vty - **line vty**
Paso 6. Habilitar SSH versión 2 - **ip ssh versión 2**

Para mostrar los datos de la versión y de configuración de SSH en el dispositivo que configuró como servidor SSH, use el comando show ip ssh. En el ejemplo, se habilitó la versión 2 de SSH. Para verificar las conexiones SSH al dispositivo, use el comando show ssh.

Configuración del gateway predeterminado

Si su red local sólo tiene un enrutador, será el enrutador de puerta de enlace y todos los hosts y conmutadores de su red deben estar configurados con esta información. Si la red local tiene varios enrutadores, debe seleccionar uno de ellos para que sea el enrutador de puerta de enlace predeterminado. La puerta de enlace predeterminada se usa solamente cuando el host desea enviar un paquete a un dispositivo de otra red. En general, la dirección de la puerta de enlace predeterminada es la dirección de la interfaz del enrutador conectada a la red local del host. La dirección IP del dispositivo host y la dirección de interfaz del enrutador deben estar en la misma red.

Para conectarse y administrar un conmutador a través de una red IP local, debe tener un SVI configurado. El SVI se configura con una dirección IPv4 y una máscara de subred en la LAN local. El conmutador también debe tener una dirección de puerta de enlace predeterminada configurada para administrar el conmutador de forma remota desde otra red. Para configurar una puerta de enlace predeterminada IPv4 en un conmutador, use el comando de configuración global **ip default-gateway *dirección-ip***. La *dirección IP* que se configura es la dirección IPv4 de la interfaz del enrutador local conectada al conmutador.

11.5.2 Webster - Preguntas de Reflexión

Es bueno tener un poco de ayuda cuando se tiene un gran proyecto, como lo tiene Diego. Este módulo tiene casi todo lo que necesito saber para configurar una red de sucursales. Según lo que han aprendido en este curso hasta ahora, apuesto a que podrían haber ayudado a Diego. ¿Tiene acceso a una red lo suficientemente grande como para contener switches y más de un router? Si es así, pregunte a su departamento de TI si podría hacer un recorrido. ¡Es posible que se sorprenda de lo que ya comprende!

11.5.3 Prueba de Crear una Pequeña Red de Cisco

Un usuario puede imprimir en una impresora que está en la misma red, pero el tráfico del usuario no puede alcanzar Internet. ¿Cuál de las siguientes opciones es una causa posible del problema?

- La dirección del puerta de enlace predeterminada es incorrecta o no existe. ☺←
- La dirección IP de la PC no es correcta.
- El cable de red conectado a la PC del usuario está defectuoso.
- La NIC de la PC está defectuosa.

¿Qué conexión proporciona una sesión de CLI segura con cifrado a un conmutador Cisco?

- una conexión de la consola
- una conexión AUX
- una conexión Telnet
- una conexión SSH ☺←

¿En qué interfaz de switch configuraría un administrador una dirección IP, de modo que sea posible administrar el switch de forma remota?

- FastEthernet0/1
- VLAN 1 ☺←
- vty 0
- console 0

Un administrador definió una cuenta de usuario local con una contraseña secreta en el router R1 para usarla con SSH. ¿Qué tres pasos adicionales se requieren para configurar R1 para aceptar solo conexiones SSH cifradas? (Escoja tres opciones).

- Configurar el nombre de dominio IP en el enrutador. ☺←
- Habilitar las sesiones Telnet de entrada VTY.
- Generar las claves SSH. ☺←
- Configurar el DNS en el enrutador.
- Habilitar las sesiones SSH de entrada vty. ☺←
- Generar claves pre compartidas bidireccionales.

Relaciona los comandos con las acciones correctas.

muestra un mensaje después de acceder al enrutador	✓ banner motd
brinda seguridad en la consola	✓ password class
configura un nombre en el enrutador	✓ hostname

Un técnico está configurando un router para permitir todas las formas de acceso de administración. Como parte de cada tipo de acceso diferente, el técnico está intentando escribir el comando login. ¿Qué modo de configuración se debe introducir para realizar esta tarea?

- modo EXEC del usuario
- modo de configuración global
- modo de configuración de líneas ☺←
- modo EXEC privilegiado

Explique: El comando **login** se utiliza para permitir el acceso a un router o conmutador a través de líneas auxiliares, líneas de consola y líneas Telnet.

¿Qué enunciado describe las SVI?

- Se crea automáticamente un SVI para cada VLAN en un switch multicapa.
- Al crear un SVI se crea automáticamente una VLAN asociada.
- Se crea un SVI predeterminado para la VLAN 1 para la administración del switch. ☺←
- Un SVI solo se puede crear para fines de administración.

Explique: Para permitir la administración remota del switch, se crea un SVI de forma predeterminada para la VLAN 1

¿Cuál es la diferencia entre usar Telnet o SSH a fin de conectarse a un dispositivo de red para fines administrativos?

- Telnet utiliza UDP como protocolo de transporte, mientras que SSH utiliza TCP.
- Telnet no proporciona autenticación, mientras que SSH sí lo hace.

Telnet admite una GUI de hosts, mientras que SSH solo admite una CLI de hosts.
Telnet envía un nombre de usuario y una contraseña en texto sin formato, mientras que SSH cifra el nombre de usuario y la contraseña. ☺←

¿Qué tipo de acceso está asegurado en un enrutador o conmutador de Cisco con el comando **enable secret**?

Terminales virtuales	EXEC con privilegios ☺←
Puerto auxiliar	Línea de consola

¿Qué declaración con respecto al comando **service password-encryption** es verdadera?

Está configurado en modo EXEC privilegiado.
Cifra solo contraseñas en modo de línea.
Tan pronto como se introduce el comando service password-encryption, se cifran todas las contraseñas establecidas actualmente que se mostraban en texto sin formato. ☺←
Para ver las contraseñas cifradas por el comando service password-encryption en texto sin formato, ejecute el comando **no service password-encryption.**

¿Qué sucede cuando se ingresa el comando **transport input ssh** en las líneas vty del conmutador?

Se habilita el cliente SSH en el conmutador.
La comunicación entre el conmutador y los usuarios remotos está cifrada. ☺←
El conmutador requiere una combinación de nombre de usuario/contraseña para el acceso remoto.
El conmutador requiere conexiones remotas a través de un software cliente propietario.

Módulo 12: ICMP Protocolos de Mensajes de Control de Internet

0. Introducción

12.0.1 Webster: ¿Por Qué Debería Tomar este Módulo?

Felicitaciones. ¡Ha llegado al último módulo de este curso! Mi amigo, Diego, ha configurado la red y ahora debe asegurarse de que funcione correctamente. Afortunadamente, hay algunas herramientas que él y usted pueden utilizar para detectar fácilmente si hay algún problema con su red. En este módulo, aprenderá a usar esas herramientas para solucionar problemas de su propia red. ¡Esto será divertido!

12.0.2 ¿Qué Aprenderé en este Módulo?

- **Título del Módulo**: ICMP
- **Objetivo del Módulo**: Usar varias herramientas para probar la conectividad de la red.

Título del Tema	Objetivo del Tema
Mensajes ICMP	Explique la forma en que se usa ICMP para probar la conectividad de red
Pruebas de ping y traceroute	Utilice las utilidades de ping y traceroute para probar la conectividad de red.

1. Mensajes ICMP

12.1.1 Mensajes ICMPv4 e ICMPv6

En este tema, aprenderá acerca de los diferentes tipos de ***Protocolos de Mensajes de Control de Internet - ICMP*** y las herramientas que se utilizan para enviarlos.

Aunque IP es sólo un protocolo de mayor esfuerzo, el conjunto ***TCP/IP*** proporciona *mensajes de error* y *mensajes informativos* cuando se comunica con otro dispositivo IP. Estos mensajes se envían mediante los servicios de ICMP. El objetivo de estos mensajes no es hacer que IP sea confiable sino proporcionar respuestas acerca de temas relacionados con el procesamiento de paquetes IP en determinadas condiciones,. Los mensajes de ICMP no son obligatorios y, a menudo, no se permiten dentro de una red por razones de seguridad.

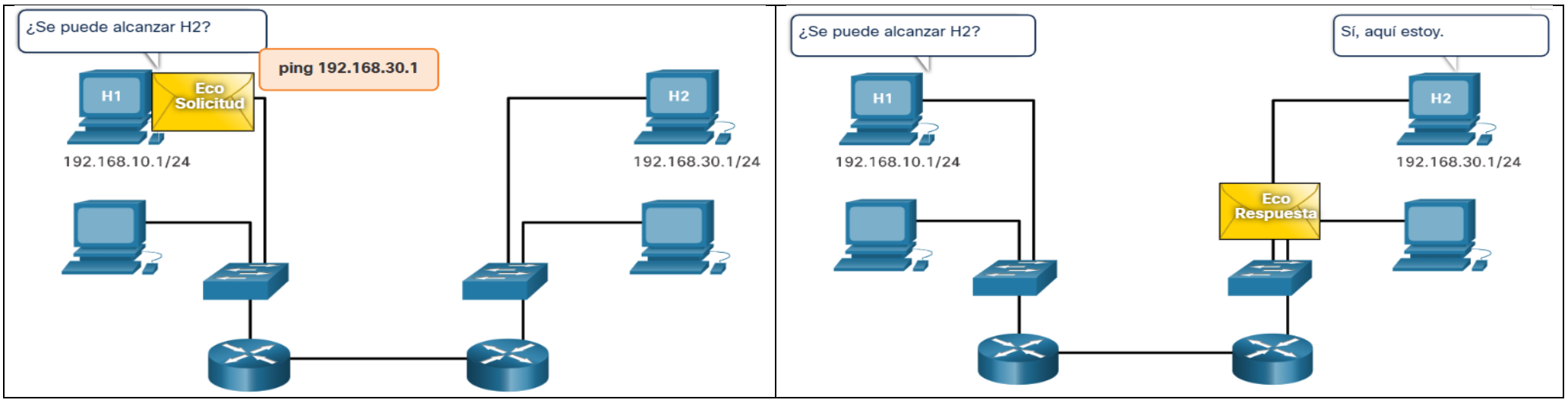
El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional. En este curso, el término ICMP se utilizará para referirse tanto a ICMPv4 como a ICMPv6.

Los tipos de mensajes ICMP y las razones por las que se envían son extensos. Los mensajes ICMP comunes a ICMPv4 e ICMPv6 y discutidos en este módulo incluyen:

- Accesibilidad al host
- Destino o servicio inaccesible
- Tiempo superado

12.1.2 Accesibilidad del Host

Se puede utilizar un mensaje de eco ICMP para probar la accesibilidad de un host en una red IP. El host local envía una solicitud de eco ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco. Este uso de los mensajes ***ICMP Echo*** es la base de la utilidad **ping**.



12.1.3 Destino o Servicio Inalcanzable

Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje ICMP de destino inalcanzable para notificar al origen que el destino o el servicio son inalcanzables. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete.

Algunos de los códigos de destino inalcanzable para ICMPv4 son los siguientes:

- 0 - Red inalcanzable
- 1 - Host inalcanzable
- 2 - Protocolo inalcanzable
- 3 - Puerto inalcanzable

Algunos de los códigos de destino inalcanzable para ICMPv6 son los siguientes:

- 0 - No hay ruta para el destino
- 1 - La comunicación con el destino está prohibida administrativamente (por ejemplo, firewall)
- 2 - Más allá del alcance de la dirección de origen
- 3 - No se puede alcanzar la dirección
- 4 - Puerto inalcanzable

Nota: ICMPv6 tiene códigos similares, pero levemente diferentes para los mensajes de destino inalcanzable.

12.1.4 Tiempo Excedido

Los routers utilizan los mensajes de ***tiempo excedido*** de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo Tiempo de Vida (TTL) del paquete disminuyó a 0. Si un router recibe un paquete y disminuye el campo TTL en el paquete IPV4 a cero, descarta el paquete y envía un mensaje de ***tiempo excedido*** al host de origen.

ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. En lugar del campo TTL de IPv4, ICMPv6 usa el campo ***Límite de Salto*** de IPv6 para determinar si el paquete ha expirado.

Nota: Los mensajes de ***tiempo excedido*** son utilizados por la herramienta **traceroute**.

12.1.5 Mensajes ICMPv6

Los mensajes informativos y de error que se encuentran en ICMPv6 son muy similares a los mensajes de control y de error que implementa ICMPv4. Sin embargo, ICMPv6 tiene nuevas características y funcionalidad mejorada que no se encuentran en ICMPv4. Los mensajes ICMPv6 están encapsulados en IPv6. ICMPv6 incluye cuatro mensajes nuevos como parte del ***Protocolo de Detección de Vecino - NDP***.

Los mensajes entre un router IPv6 y un dispositivo IPv6, incluida la asignación dinámica de direcciones, son los siguientes:

- Mensaje de solicitud de router (RS)
- Mensaje de anuncio de router (RA)

Los mensajes entre dispositivos IPv6, incluida la detección de direcciones duplicadas y la resolución de direcciones, son los siguientes:

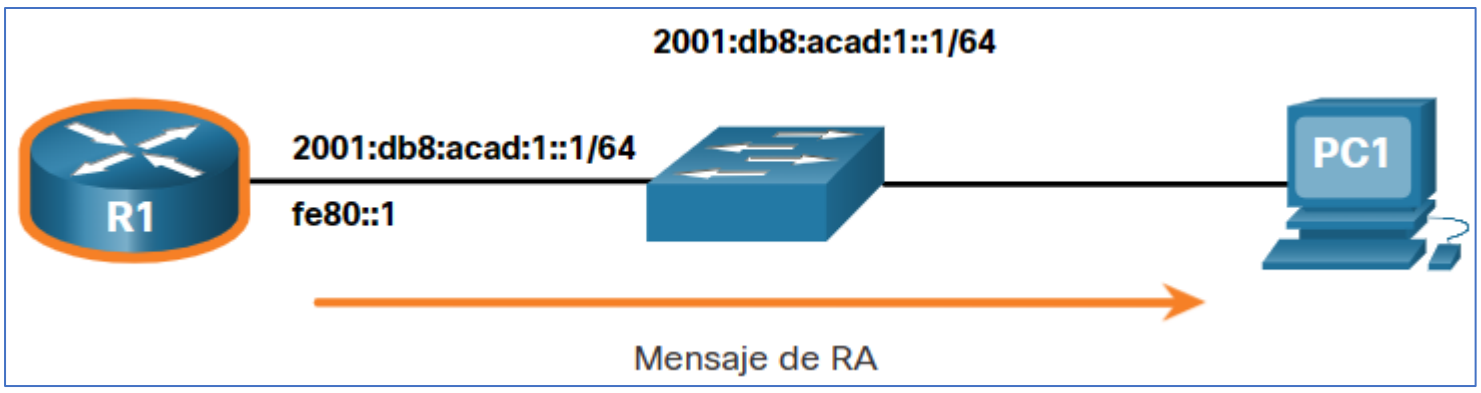
- Mensaje de solicitud de vecino (NS)
- Mensaje de anuncio de vecino (NA)

Nota: El ND de ICMPv6 también incluye el mensaje de redireccionamiento, que tiene una función similar al mensaje de redireccionamiento utilizado en ICMPv4.

Mensajes de anuncio de router - RA

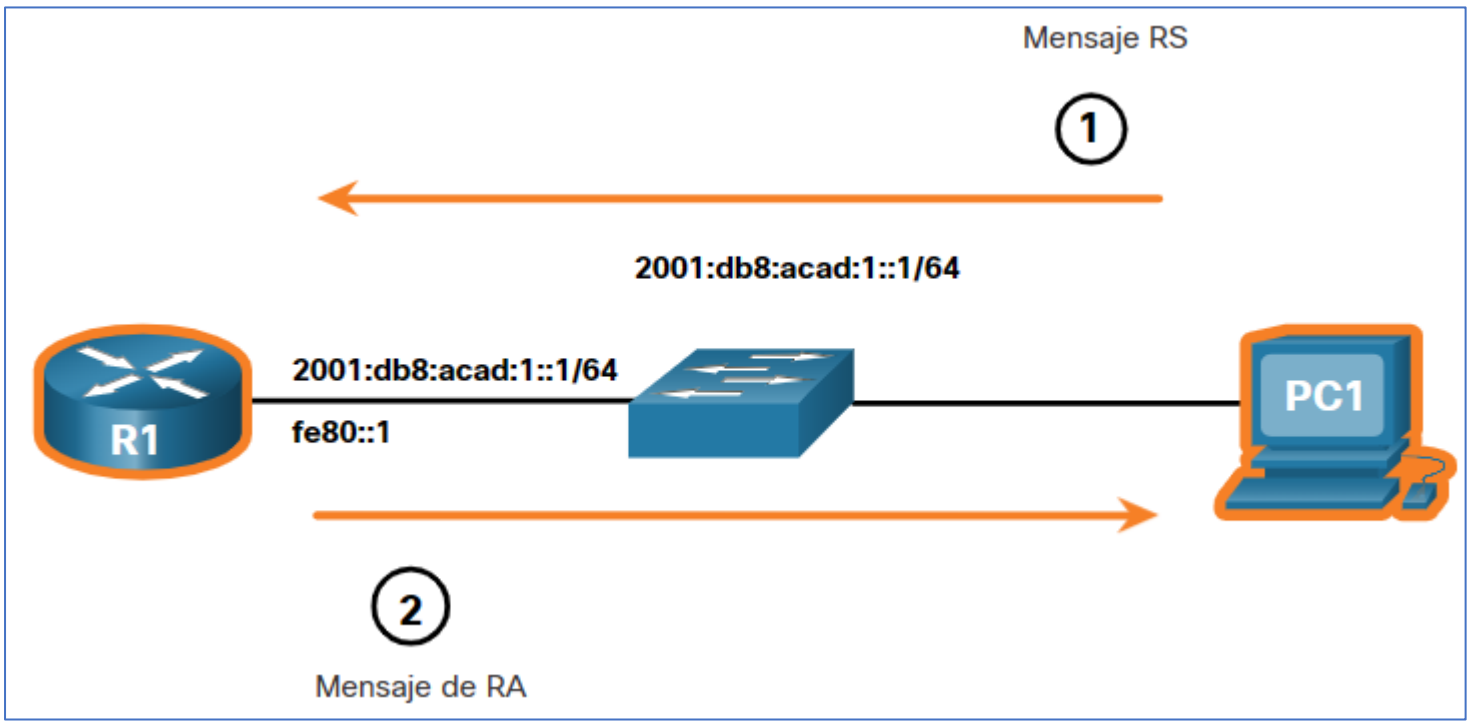
Los enrutadores habilitados para IPv6 envían mensajes de RA cada 200 segundos para proporcionar información de direccionamiento a los hosts habilitados para IPv6. El mensaje RA incluye información de direccionamiento para el host, como el prefijo, la longitud del prefijo, la dirección DNS y el nombre de dominio. Un host que utiliza la ***Configuración Automática de Direcciones sin Estado - SLAAC*** establecerá su puerta de enlace predeterminada en la dirección de enlace local del enrutador que envió el RA.

R1 envía un mensaje de RA: «Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear una dirección de unidifusión global IPv6. El prefijo es 2001:db8:acad:1: :/64. Por cierto, use mi dirección local de enlace fe80: :1 como su puerta de enlace predeterminada. «



Mensajes de solicitud de router - RS
Un router habilitado para IPv6 también enviará un mensaje RA en respuesta a un mensaje RS. En la figura, PC1 envía un mensaje RS para determinar cómo recibir dinámicamente su información de dirección IPv6. R1 responde a la RS con un mensaje de RA.

1. PC1 envía un mensaje RS, «Hola, acabo de arrancar. ¿Hay un router IPv6 en la red? Necesito saber cómo obtener la información de mi dirección IPv6 de forma dinámica».
2. R1 responde con un mensaje de RA. «Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear una dirección de unidifusión global IPv6. El prefijo es 2001:db8:acad:1::/64. Por cierto, use mi dirección local de enlace fe80::1 como su puerta de enlace predeterminada.»

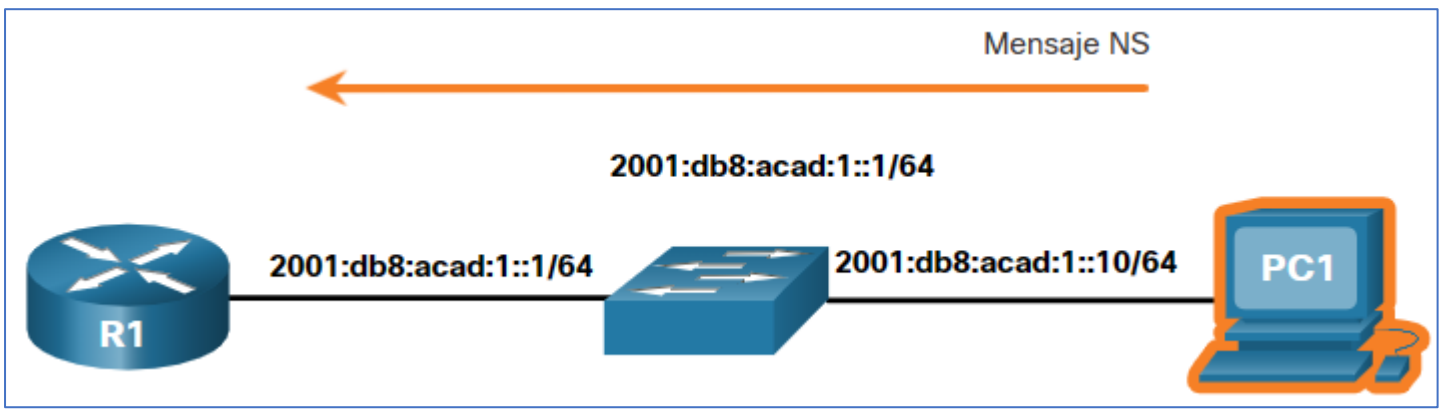


Mensajes de Solicitud de Vecino - NS
Cuando a un dispositivo se le asigna una dirección de unidifusión global IPv6 o unidifusión local de enlace, puede realizar una ***Detección de Dirección Duplicada - DAD*** para garantizar que la dirección IPv6 sea única. Para verificar la unicidad de una dirección, el dispositivo enviará un mensaje NS con su propia dirección IPv6 como la dirección IPv6 objetivo, como se muestra en la figura.

Si otro dispositivo de la red tiene esta dirección, responde con un mensaje de ***Anuncio de Vecino - NA***. Este mensaje NA notifica al dispositivo emisor que la dirección está en uso. Si no se devuelve un mensaje NA correspondiente dentro de un cierto período de tiempo, la dirección de unidifusión es única y aceptable para su uso.

Nota: No se requiere DAD, pero RFC 4861 recomienda que DAD se realice en direcciones de unidifusión.

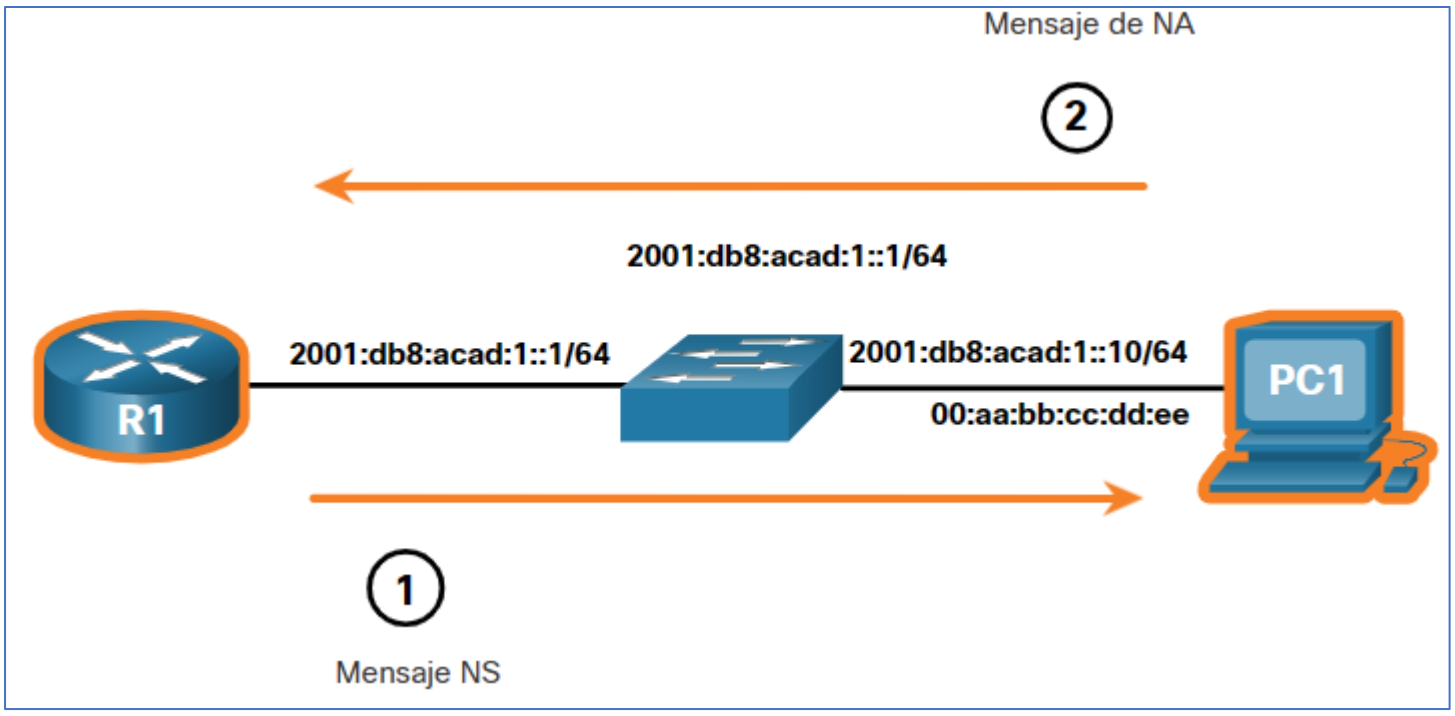
PC1 envía un mensaje NS para comprobar que una dirección sea única, «¿Quién tiene la dirección IPv6 2001:db8:acad:1::10, envíeme su dirección MAC?»



Mensaje de Anuncio de Vecino - NA
La resolución de direcciones se utiliza cuando un dispositivo en la LAN conoce la dirección IPv6 de unidifusión de un destino, pero no conoce la dirección MAC de Ethernet. Para determinar la dirección MAC del destino, el dispositivo envía un mensaje de NS a la dirección de nodo solicitado. El mensaje incluye la dirección IPv6 conocida (objetivo). El dispositivo que se destinó a la dirección IPv6 responde con un mensaje NA que contiene la dirección MAC de Ethernet.

En la figura, R1 envía un mensaje NS a 2001:db8:acad:1: :10 pidiendo su dirección MAC.

1. R1 envía un mensaje NS de resolución de dirección. «¿Quién tiene la dirección IPv6 2001:db8:acad:1::10, envíeme su dirección MAC?»
2. PC1 responde con un mensaje NA. «Soy 2001:db8:acad:1::10 y mi dirección MAC es 00:aa:bb:cc:dd:ee.»



12.1.6 Verifique su Comprensión - Mensajes ICMP

¿Qué dos tipos de mensajes ICMP son comunes a ICMPv4 e ICMPv6? (Elija dos opciones).

Destino o servicio inaccesible ☺←
Resolución de nombre de host
Configuración de IP
Origen inalcanzable
Tiempo superado ☺←

Los mensajes ICMP comunes a ICMPv4 e ICMPv6 incluyen confirmación del host, destino o servicio inalcanzable y tiempo excedido.

¿Qué tipo de mensaje ICMPv6 enviaría un host para adquirir una configuración IPv6 al arrancar?

Mensaje de anuncio de vecino (NA)	Mensaje de solicitud de vecino (NS)
Mensaje de anuncio de Router (RA)	Mensaje de solicitud de router (RS) ☺←

El arranque de un host habilitado para IPv6 enviaría un mensaje de solicitud de enrutador ICMPv6. Un enrutador habilitado para IPv6 respondería con un mensaje de anuncio de enrutador.

2. Pruebas de ping y traceroute

12.2.1 Ping - Probar la Conectividad

En el tema anterior, se le presentaron las herramientas **ping** y traceroute (**tracert**). En este tema, aprenderá acerca de las situaciones en las que se usa cada herramienta y cómo usarlas. Ping es una utilidad de prueba de IPv4 e IPv6 que utiliza la solicitud de eco ICMP y los mensajes de respuesta de eco para probar la conectividad entre hosts.

Para probar la conectividad con otro host de una red, se envía una solicitud de eco a la dirección de host mediante el comando **ping**. Si el host en la dirección especificada recibe la solicitud de eco, responde con una respuesta de eco. A medida que se recibe cada respuesta de eco, el comando **ping** proporciona comentarios acerca del tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta. Esto puede ser una medida del rendimiento de la red.

El comando ping tiene un valor de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro del tiempo de espera, el comando ping proporciona un mensaje que indica que no se recibió una respuesta. Esto puede indicar que hay un problema, pero también podría indicar funciones de seguridad habilitadas en la red que bloquean los mensajes de ping. Es común que el primer ping se agote si es necesario realizar la resolución de direcciones (ARP o ND) antes de enviar la solicitud de eco ICMP.

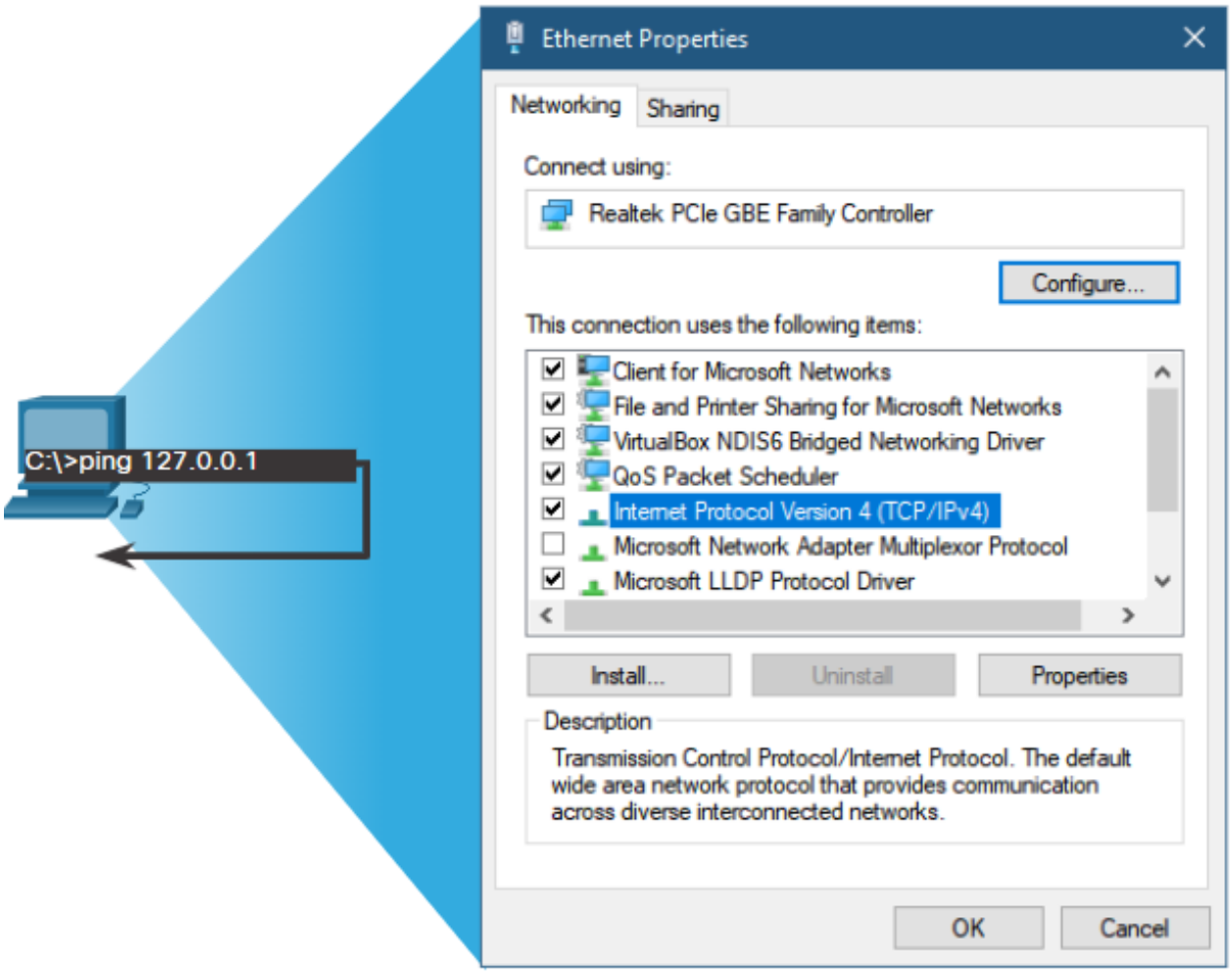
Una vez que se envían todas las solicitudes, la utilidad **ping** proporciona un resumen que incluye la tasa de éxito y el tiempo promedio del viaje de ida y vuelta al destino. Los tipos de pruebas de conectividad que se realizan con **ping** son los siguientes:

- Hacer ping al loopback local
- Hacer ping a la puerta de enlace predeterminada
- Hacer ping al host remoto

12.2.2 Hacer Ping al Loopback

Ping se puede usar para *probar la configuración interna* de IPv4 o IPv6 del host local. Para realizar esta prueba, se debe hacer **ping** a la dirección de loopback local 127.0.0.1 para IPv4 (::1 para IPv6). Una respuesta de 127.0.0.1 para IPv4 (o ::1 para IPv6) indica que IP está instalado correctamente en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no indica que las direcciones, las máscaras o los gateways estén configurados adecuadamente. Tampoco indica nada acerca del estado de la capa inferior de la pila de red. Simplemente, prueba el protocolo IP en la capa de red de dicho protocolo. Un mensaje de error indica que TCP/IP no funciona en el host.

- Hacer ping al host local permite confirmar que el protocolo TCP/IP se encuentra instalado en el host y que funciona.
- Hacer ping a 127.0.0.1 ocasiona que un dispositivo se haga ping a sí mismo.



12.2.3 Hacer Ping a la Puerta de Enlace Predeterminada

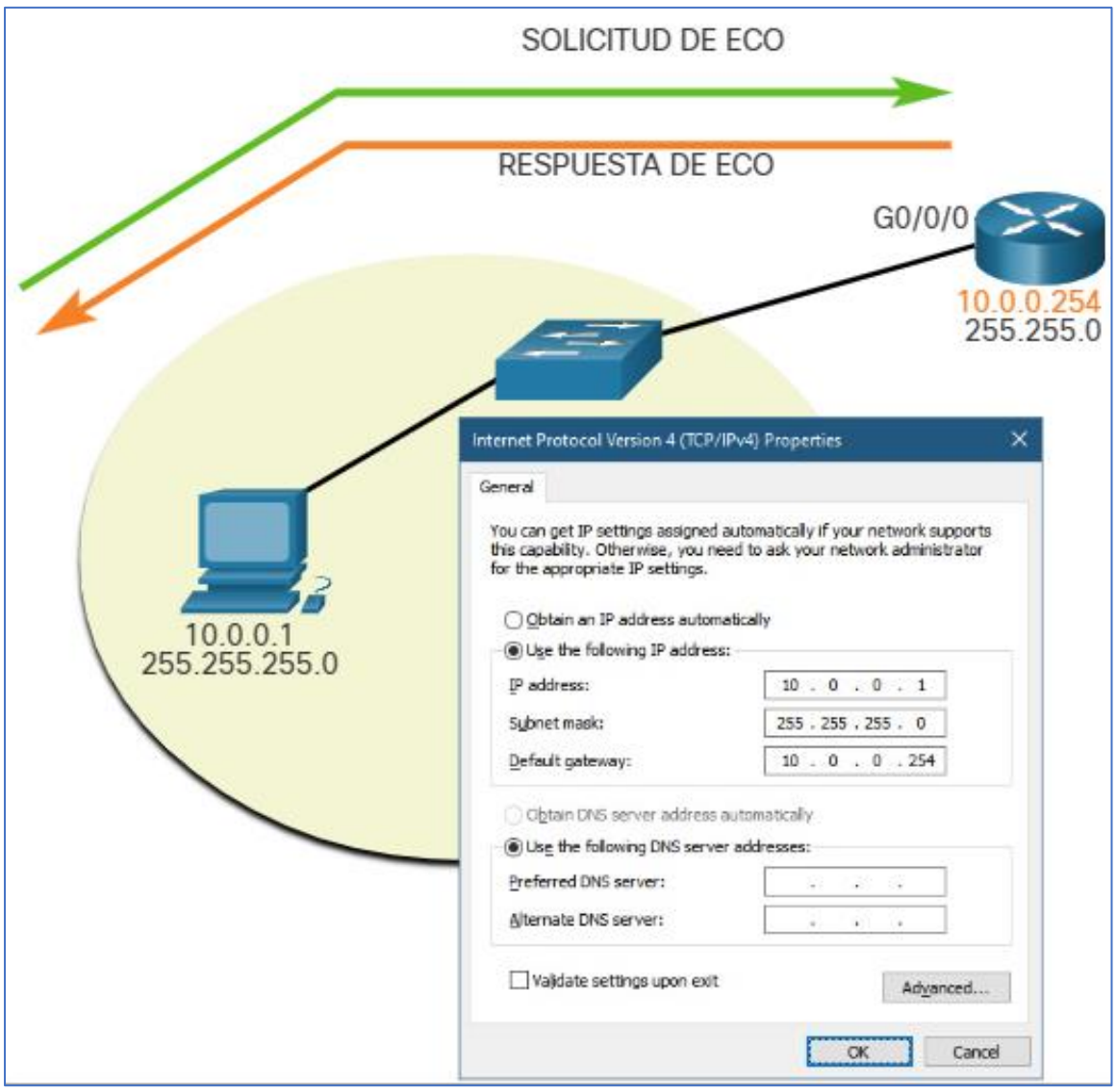
También es posible utilizar el comando **ping** para *probar* la *capacidad de comunicación* de un host en la red local. Esto generalmente se hace haciendo ping a la dirección IP de la puerta de enlace predeterminada del host. Un **ping** exitoso a la puerta de enlace predeterminada indica que el host y la interfaz del enrutador que sirve como puerta de enlace predeterminada están operando en la red local.

Para esta prueba, la dirección de puerta de enlace predeterminada se usa con mayor frecuencia porque el router normalmente siempre está operativo. Si la dirección de puerta de enlace predeterminada no responde, se puede enviar un **ping** a la dirección IP de otro host en la red local que se sabe que está operativo.

Si la puerta de enlace predeterminada u otro host responde, entonces el host local puede comunicarse con éxito a través de la red local. Si la puerta de enlace predeterminada no responde, pero otro host sí, esto podría indicar un problema con la interfaz del router que funciona como la puerta de enlace predeterminada.

Una posibilidad es que se haya configurado una dirección de puerta de enlace predeterminada incorrecta en el host. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, *pero se le ha aplicado seguridad*, de manera que no procesa o responde solicitudes de ping.

El host hace ping a su puerta de enlace predeterminada, enviando una solicitud de eco ICMP. La puerta de enlace predeterminada envía una respuesta de eco confirmando la conectividad.

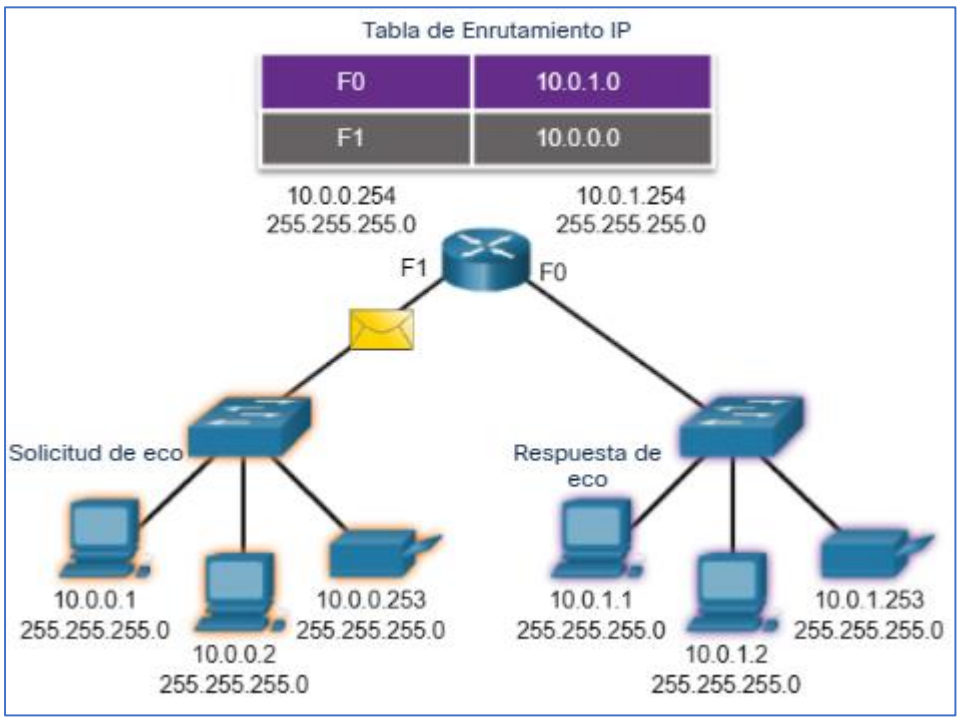


12.2.4 Hacer Ping a un Host Remoto

También se puede utilizar el comando ping para probar la capacidad de un host local para comunicarse en una *interconexión de redes*. El host local puede hacer ping a un host IPv4 operativo de una red remota, como se muestra en la ilustración. El router utiliza su tabla de enrutamiento IP para reenviar los paquetes.

Si este ping se realiza correctamente, se puede verificar el funcionamiento de una amplia porción de la interconexión de redes. Un **ping** exitoso a través de la red confirma la comunicación en la red local, el funcionamiento del enrutador que sirve como puerta de enlace predeterminada y el funcionamiento de todos los demás enrutadores que podrían estar en la ruta entre la red local y la red del host remoto. Además, se puede verificar la funcionalidad del host remoto. Si el host remoto no pudiera comunicarse fuera de su red local, no habría respondido.

Nota: Muchos administradores de redes limitan o prohíben la entrada de mensajes ICMP a la red de la empresa; por lo tanto, la falta de una respuesta de **ping** puede ser por razones de seguridad.



12.2.5 Traceroute - Probar el Camino

El comando ping se usa para probar la conectividad entre dos hosts, pero no proporciona información sobre los detalles de los dispositivos entre los hosts. Traceroute (***tracert***) es una utilidad que genera una lista de saltos alcanzados correctamente a lo largo de la ruta. Esta lista puede proporcionar información importante para la solución de problemas. Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en la ruta entre los hosts. Si los datos fallan en algún salto a lo largo del camino, la dirección del último router que respondió al rastreo nos indicará dónde se encuentra el problema o restricciones de seguridad existentes.

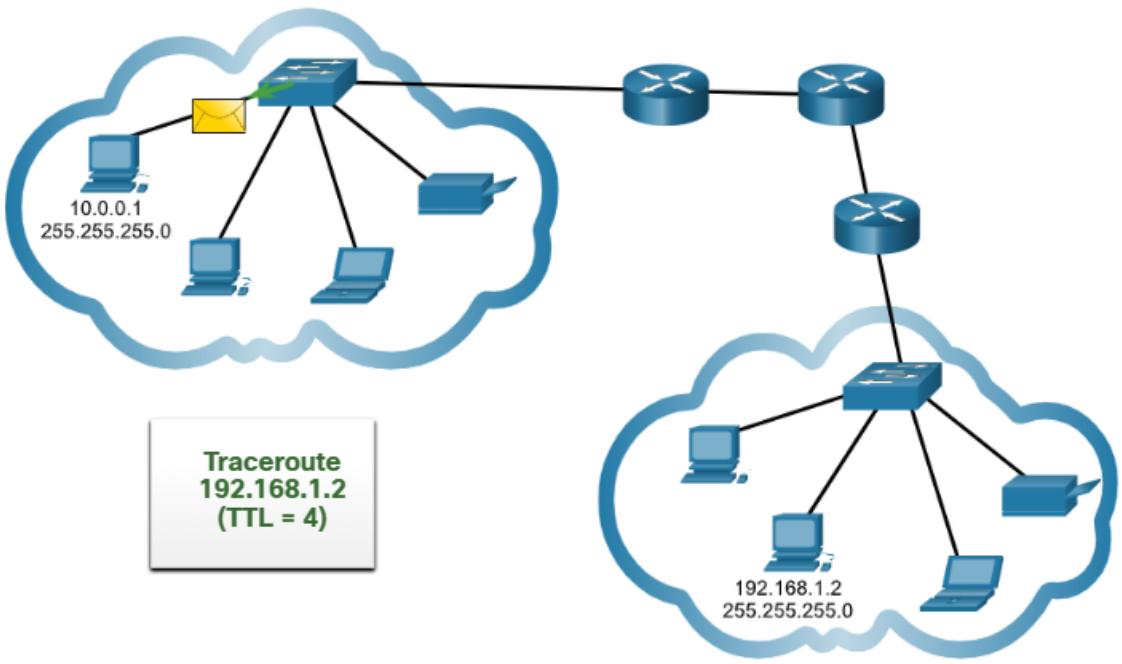
Tiempo de Ida y Vuelta (RTT)

Traceroute proporciona el tiempo de ida y vuelta para cada salto a lo largo del camino e indica si un salto no responde. El tiempo de ida y vuelta es el tiempo que tarda un paquete en llegar al host remoto y que la respuesta del host regrese. Se utiliza un asterisco **(*)** para indicar un paquete perdido o sin respuesta.

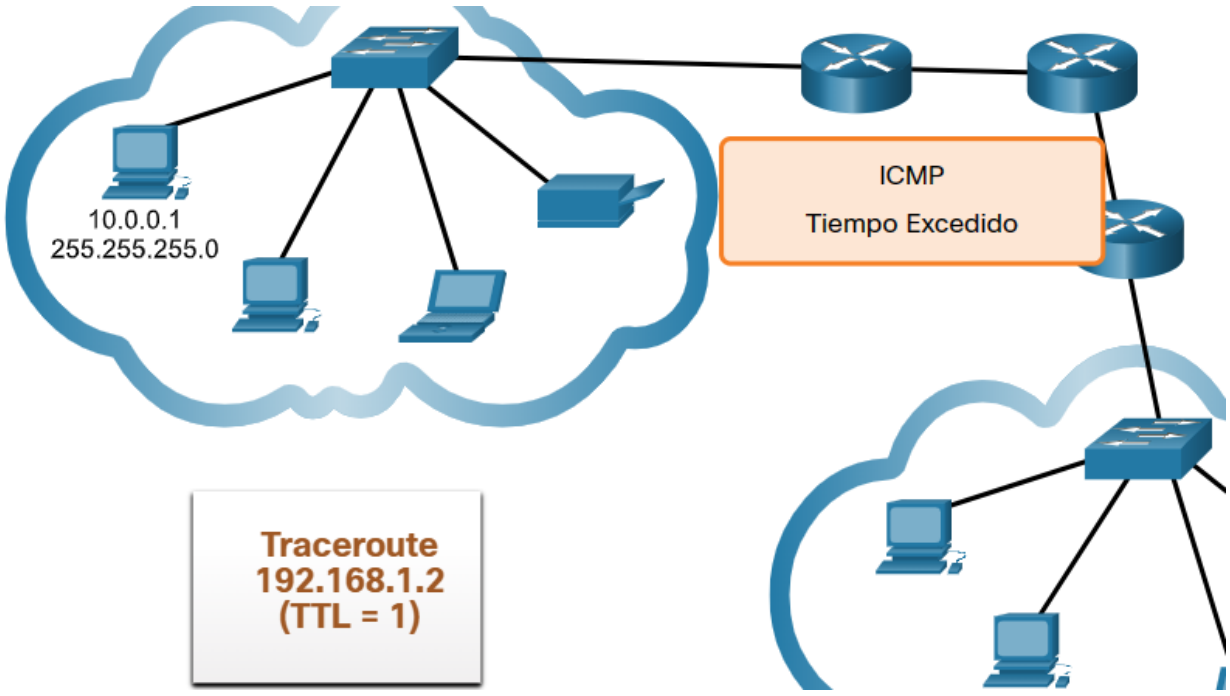
Esta información se puede usar para localizar un router problemático en la ruta o si está configurado para no responder. Si en la pantalla se muestran tiempos de respuesta elevados o pérdidas de datos de un salto en particular, esto es un indicio de que los recursos del router o sus conexiones pueden estar sobrecargados.

TTL de IPv4 y Límite de Saltos de IPv6

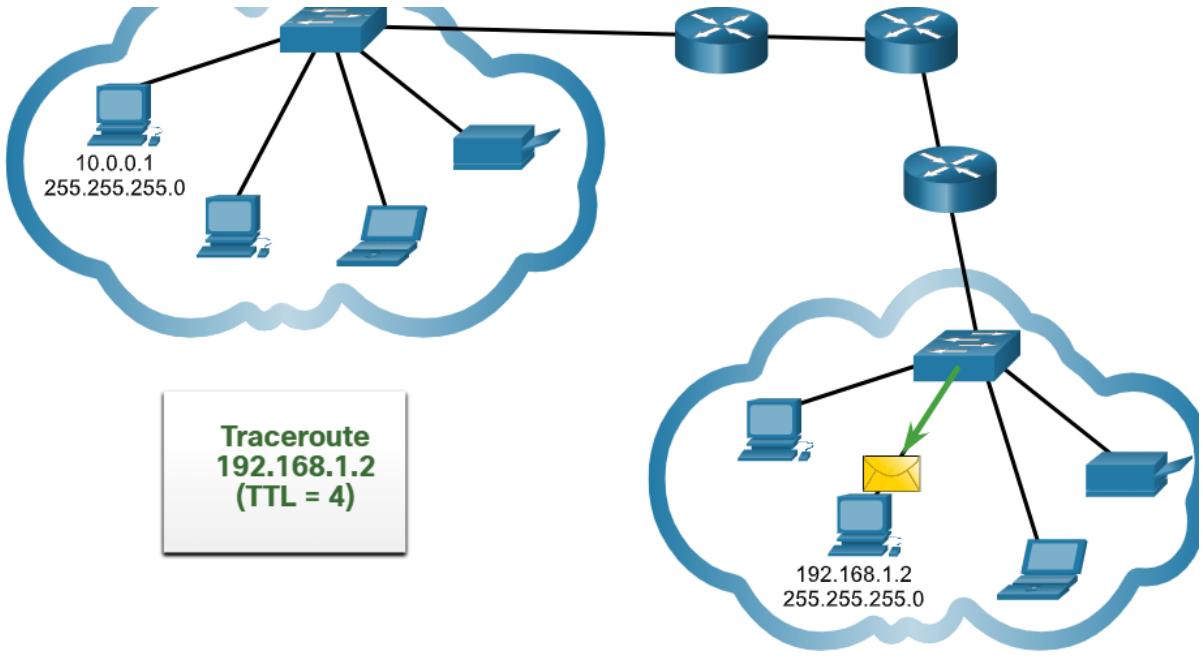
Traceroute utiliza una función del campo TTL en IPv4 y el campo Límite de Salto en IPv6 en los encabezados de Capa 3, junto con el mensaje de ICMP Tiempo Excedido.



La primera secuencia de mensajes enviados desde traceroute tiene un valor de 1 en el campo TTL. Esto hace que el TTL agote el tiempo de espera del paquete IPv4 en el primer router. Este router responde con un mensaje ICMPv4 Tiempo Excedido. Traceroute ahora tiene la dirección del primer salto.



A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. Esto proporciona el rastro con la dirección de cada salto a medida que los paquetes caducan más adelante en la ruta. El campo TTL sigue aumentando hasta que se alcanza el destino, o se incrementa a un máximo predefinido.



Una vez que se alcanza el destino final, el host responde con un mensaje de puerto inalcanzable ICMP o un mensaje de respuesta de eco ICMP en lugar del mensaje TTL ICMP de tiempo excedido.

12.2.6 Packet Tracer - Verificar el Direccionamiento IPv4 e IPv6

En esta actividad, cumplirá los siguientes objetivos:

- Pruebe y restaure la conectividad IPv4
- Pruebe y restaure la conectividad IPv6

Objetivos

- **Parte 1: Completar la documentación de la tabla de direccionamiento**
- **Parte 2: Probar la conectividad mediante el comando ping**
- **Parte 3: Descubrir la ruta mediante su rastreo**

Aspectos básicos

La técnica ***dual-stack*** permite que IPv4 e IPv6 coexistan en la misma red. En esta actividad, investigará la implementación de una técnica dual-stack, incluidos la documentación de la configuración de IPv4 e IPv6 para terminales, la prueba de conectividad para IPv4 e IPv6 mediante el comando **ping** y el rastreo de la ruta de terminal a terminal para IPv4 e IPv6.

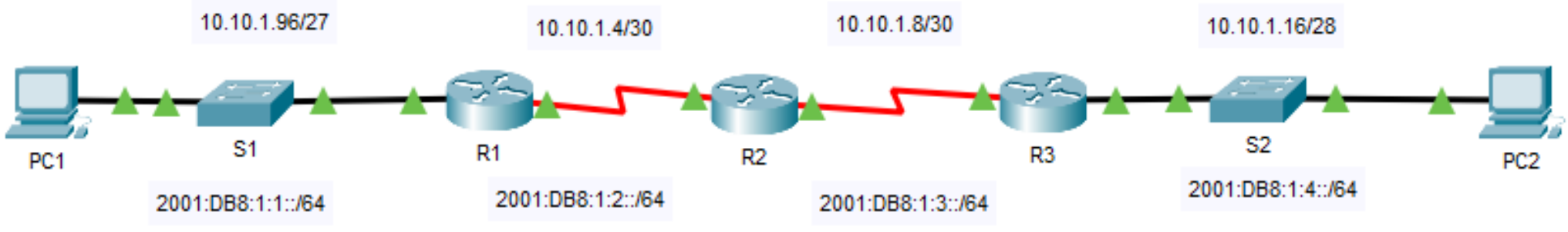


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP / Prefijo		Puerta de enlace predeterminada
R1	G0/0	10.10.1.97	255.255.255.224	N/D
		2001:db 8:1:1: :1/64		
	S0/0/1	10.10.1.6	255.255.255.252	N/D
		2001:db 8:1:2: :2/64		
		fe80::1		
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:db8:1:2::1/64		
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:db8:1:3::1/64		
		fe80::2		
R3	G0/0	10.10.1.17	255.255.255.240	N/A
		2001:db 8:1:4: :1/64		
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:db8:1:3::2/64		
		fe80::3		
PC1	NIC	10.10.1.100	255.255.255.224	10.10.1.97
		2001:db 8:1:1: :a/64		fe80::1
PC2	NIC	10.10.1.20	255.255.255.240	10.10.1.17
		2001:db 8:1:4: :a/64		fe80::3

Parte 1: Completar la documentación de la tabla de direccionamiento

Paso 1: Usar el comando ***ipconfig*** para verificar el direccionamiento IPv4.

a. Haga Click en **PC1** y abra el **Command Prompt**.

b. Introduzca el comando **ipconfig /all** para obtener la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

c. Haga Click en **PC2** y abra el **Command Prompt**.

d. Introduzca el comando **ipconfig /all** para obtener la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

Paso 2: Usar el comando ***ipv6config*** para verificar el direccionamiento IPv6.

a. En la **PC1**, introduzca el comando **ipv6config /all** para obtener la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.

b. En la **PC2**, introduzca el comando **ipv6config /all** para obtener la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.

Parte 2: Probar la conectividad mediante el comando ping

Paso 1: Usar el comando ping para verificar la conectividad IPv4.

a. En la **PC1**, haga ping a la dirección IPv4 de la **PC2**. ¿El resultado fue correcto? **Si.**

b. En la **PC2**, haga ping a la dirección IPv4 de la **PC1**. ¿El resultado fue correcto? **Si.**

Paso 2: Usar el comando ping para verificar la conectividad IPv6.

a. En la **PC1**, haga ping a la dirección IPv6 de la **PC2**. ¿El resultado fue correcto? **Si.**

b. En la **PC2**, haga ping a la dirección IPv6 de la **PC1**. ¿El resultado fue correcto? **Si.**

Parte 3: Descubrir la ruta mediante su rastreo

Paso 1: Usar el comando ***tracert*** para descubrir la ruta IPv4.

a. En la **PC1**, rastree la ruta a la **PC2**.

PC> **`tracert 10.10.1.20`** ¿Qué direcciones se encontraron en el camino? **10.10.1.97, 10.10.1.5, 10.10.1.10, 10.10.1.20**

¿A qué interfaces se asocian las cuatro direcciones? **G0/0 del R1, S0/0/0 en el R2, S0/0/01 en el R3, NIC de la PC2**

b. En la **PC2**, rastree la ruta a la **PC1**.

PC> **`tracert 10.10.1.100`** ¿Qué direcciones se encontraron en el camino? **10.10.1.17, 10.10.1.9, 10.10.1.6, 10.10.1.100**

¿A qué interfaces se asocian las cuatro direcciones? **G0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, NIC de la PC1**

Paso 2: Usar el comando tracert para detectar la ruta IPv6.

a. En la **PC1**, rastree la ruta a la dirección IPv6 de la **PC2**.

PC> **`tracert 2001:db8:1:4::a`** ¿Qué direcciones se encontraron en el camino? **2001:db 8:1:1: :1, 2001:db 8:1:2: :1, 2001:db 8:1:3: :2, 2001:db 8:1:4: :a**

¿A qué interfaces se asocian las cuatro direcciones? **G0/0 de R1, S0/0/0 de r2, S0/0/1 of R3, NIC de PC2**

b. En la **PC2**, rastree la ruta a la dirección IPv6 de la **PC1**.

¿Qué direcciones se encontraron en el camino? **2001:db 8:1:4: :1, 2001:db 8:1:3: :1, 2001:db 8:1:2: :2, 2001:db 8:1:1: :a**

¿A qué interfaces se asocian las cuatro direcciones? **G0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, NIC de la PC1**

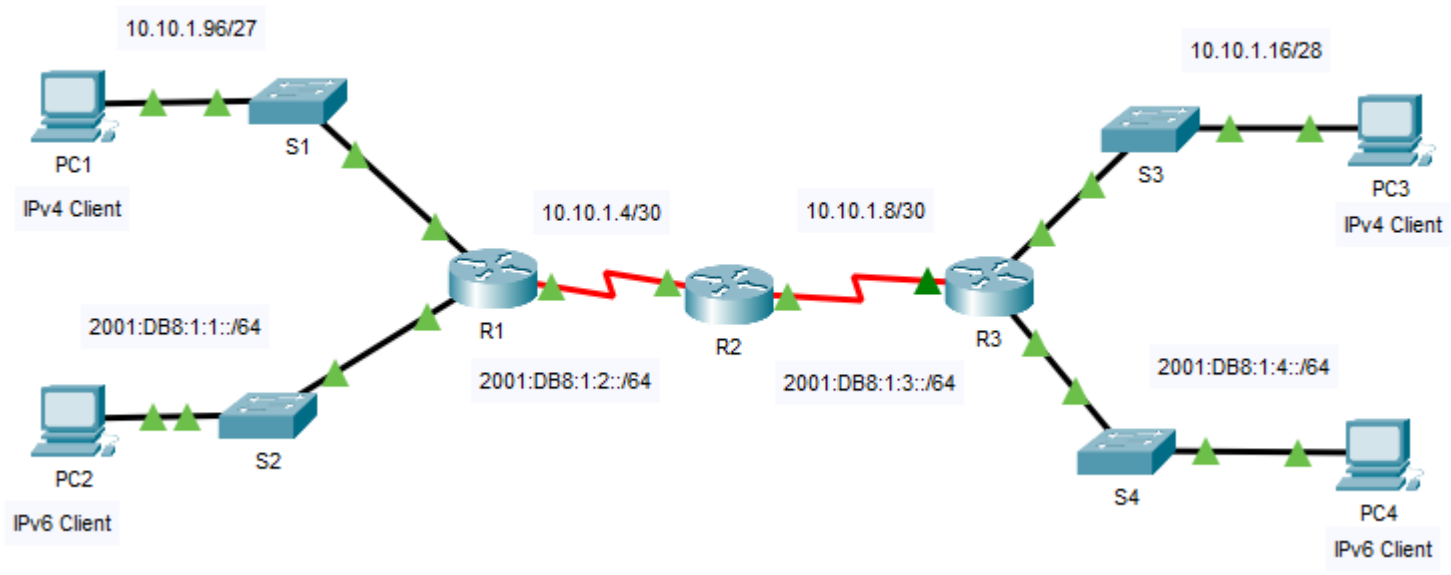
12.2.7 Packet Tracer - Usar Ping y Traceroute para Probar la Conectividad de Red

En esta actividad, cumplirá los siguientes objetivos:

- Completar la documentación de la tabla de direccionamiento
- Probar la conectividad mediante el comando ping
- Descubrir la ruta mediante su rastreo

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP / Prefijo		Puerta de enlace predeterminada
R1	G0/0	2001:db 8:1:1: :1/64		N/A
	G0/1	10.10.1.97	255.255.255.224	N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:db 8:1:2: :2/64		
		fe80::1		
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:db8:1:2::1/64		
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:db8:1:3::1/64		
		fe80::2		
R3	G0/0	2001:db 8:1:4: :1/64		N/A
	G0/1	10.10.1.17	255.255.255.240	N/A
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:db8:1:3::2/64		
		fe80::3		
PC1	NIC	10.10.1.98	255.255.255.224	10.10.1.97
PC2	NIC	2001:db 8:1:1: :2/64		fe80::1
PC3	NIC	10.10.1.18	255.255.255.240	10.10.1.17
PC4	NIC	2001:db 8:1:4: :2/64		fe80::1



Objetivos

- **Parte 1: Probar y restaurar la conectividad IPv4**
- **Parte 2: Probar y restaurar la conectividad IPv6**

Escenario

En esta actividad, hay problemas de conectividad. Además de reunir y registrar información acerca de la red, localizará los problemas e implementará soluciones razonables para restaurar la conectividad.

Nota: La contraseña de EXEC del usuario es **cisco**. La contraseña de EXEC privilegiado es **class**.

Instrucciones

Parte 1: Pruebe y restaure la conectividad IPv4

Paso 1: Utilice los comandos ipconfig y ping para verificar la conectividad.

a. Haga clic en **PC1** y abra el **símbolo del sistema**.

b. Introduzca el comando **ipconfig /all** para obtener la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

c. Haga clic en **PC3** y abra el **símbolo del sistema**.

d. Introduzca el comando **ipconfig /all** para obtener la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

e. Utilice el comando **ping** para probar la conectividad entre **PC1** y **PC3**. El ping debe fallar.

Paso 2: Localice el origen de la falla de conectividad.

a. En la **PC1**, introduzca el comando necesario para rastrear la ruta a la **PC3**. ¿Cuál es la última dirección IPv4 a la que se llegó correctamente? **10.10.1.97**

b. El rastreo finaliza después de 30 intentos. Presione **Ctrl**+**C** para detener el rastreo antes de los 30 intentos.

c. En la **PC3**, introduzca el comando necesario para rastrear la ruta a la **PC1**. ¿Cuál es la última dirección IPv4 a la que se llegó correctamente? **10.10.1.17**

d. Presione **Ctrl**+**C** para detener el rastreo.

e. Haga clic en **R1**. Presione **Enter** e inicie sesión en el router.

f. Introduzca el comando ***show ip interface brief*** para obtener una lista de las interfaces y su estado. Hay dos direcciones IPv4 en el router. Una se debe haber registrado en el paso 2a. ¿Cuál es la otra? 10.10.1.6

g. Introduzca el comando ***show ip route*** para obtener una lista de las redes a las que está conectado el router. Observe que hay dos redes conectadas a la interfaz **serial0/0/1**. ¿Cuáles son? **10.10.1.6/32, 10.10.1.4/30**

h. Repita los pasos 2e a 2g con el **R3** y registre tus respuestas. **10.10.1.10, 10.10.1.8/30, 10.10.1.10/32**

i. Haga clic en **R2**. Presione **ENTER** e inicie sesión en el router.

j. Ingrese el comando ***show ip interface brief*** y registre sus direcciones. **10.10.1.2, 10.10.1.9**

k. Ejecute más pruebas si eso permite visualizar el problema. Está disponible el modo de simulación.

Paso 3: Proponga una solución para resolver el problema

Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red. ¿Cuál es el error? **La interfaz serial 0/0/0 del R2 está configurada con una dirección IP incorrecta.** ¿Qué solución propondría para corregir el problema? **Configure la dirección IP correcta en la interfaz serial 0/0/0 del R2 (10.10.1.5)**

Paso 4: Implemente el plan

Implemente la solución que propuso en el paso 3b.

Paso 5: Verifique que la conectividad esté restaurada

a. En la **PC1**, pruebe la conectividad a la **PC3**.

b. En la **PC3**, pruebe la conectividad a la **PC1**.

¿Se solucionó el problema? **Sí.**

Paso 6: Registre la solución

Parte 2: Pruebe y restaure la conectividad IPv6

Paso 1: Utilice los comandos ipv6config y ping para verificar la conectividad.

a. Haga clic en **PC2** y abra el **símbolo del sistema**.

b. Introduzca el comando **ipv6config /all** para obtener la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.

c. Haga clic en **PC4** y abra el **símbolo del sistema**.

d. Introduzca el comando **ipv6config /all** para obtener la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.

e. Pruebe la conectividad entre la **PC2** y la **PC4**. El ping debe fallar.

Paso 2: Localice el origen de la falla de conectividad.

a. En la **PC2**, introduzca el comando necesario para rastrear la ruta a la **PC4**.

¿Cuál es la última dirección IPv6 a la que se llegó correctamente? **2001:db 8:1:3: :2**

b. El rastreo finaliza después de 30 intentos. Presione **Ctrl**+**C** para detener el rastreo antes de los 30 intentos.

c. En la **PC4**, introduzca el comando necesario para rastrear la ruta a la **PC2**.

¿Cuál es la última dirección IPv6 a la que se llegó correctamente? **No se alcanzó la dirección IPv6**

d. Presione **Ctrl**+**C** para detener el rastreo.

e. Haga clic en **R3**. Presione **Enter** (Introducir) e inicie sesión en el router.

f. Introduzca el comando **show ipv6 interface brief** para obtener una lista de las interfaces y su estado. Hay dos direcciones IPv6 en el router. Una debe coincidir con la dirección de gateway registrada en el paso 1d.

¿Hay alguna discrepancia? **Si**

g. Ejecute más pruebas si eso permite visualizar el problema. Está disponible el modo de simulación.

Paso 3: Proponga una solución para resolver el problema

Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red.

¿Cuál es el error? **La PC4 está utilizando una configuración del gateway predeterminado errónea.**

¿Qué solución propondría para corregir el problema? **Configure la PC4 con la dirección del gateway predeterminado correcta: FE80::3.**

Paso 4: Implemente el plan

Implemente la solución que propuso en el paso 3b.

Paso 5: Verifique que la conectividad esté restaurada

a. En la **PC2**, pruebe la conectividad a la **PC4**.

b. En la **PC4**, pruebe la conectividad a la **PC2**.

¿Se solucionó el problema? **Sí.**

Paso 6: Registre la solución

3. Resumen de ICMP

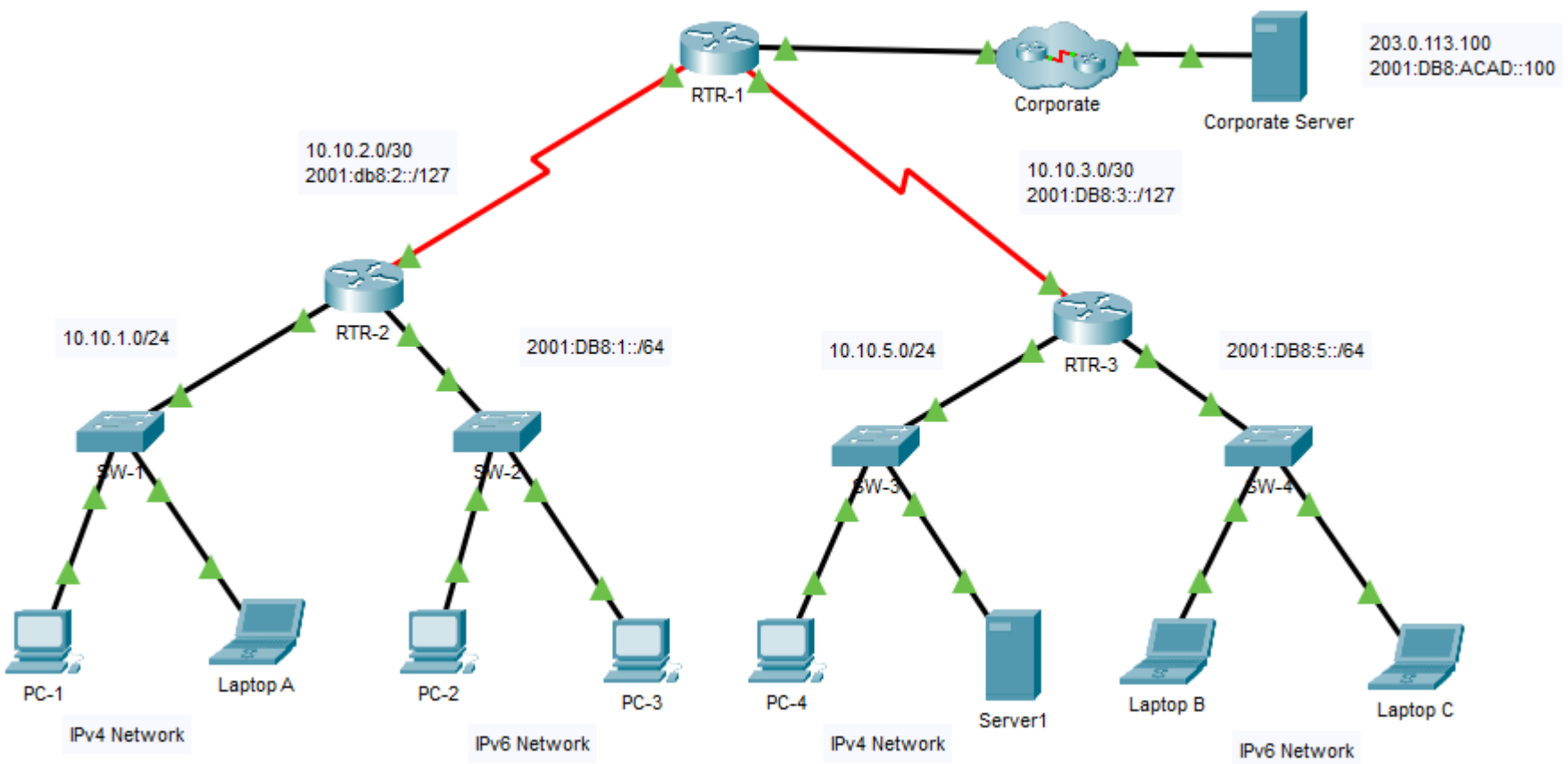
12.3.1 Packet Tracer - Utilizar ICMP para Probar y Corregir la Conectividad de Red

En esta actividad de Packet Tracer, completará los siguientes objetivos:

- Use ICMP para localizar problemas de conectividad.
- Configure los dispositivos de red para corregir problemas de conectividad.

Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección	Máscara/Prefijo	Puerta de enlace predeterminada
RTR-1	G/0/0/0	192.168.1.1	255.255.255.0	N/A
		2001:db8:4::1	/64	N/D
	S0/1/0	10.10.2.2	255.255.255.252	N/A
		2001:db8:2::2	/126	No corresponde
	/1/1	10.10.3.1	255.255.255.252	N/A
		2001:db8:3: :1	/126	No corresponde
RTR-2	G/0/0/0	10.10.1.1	255.255.255.0	N/A
	G0/0/1	2001:db 8:1: :1	/64	N/D
	S0/1/0	10.10.2.1	255.255.255.252	N/A
		2001:db 8:2: :1	/126	No corresponde
RTR-3	G0/0/0	10.10.5.1	255.255.255.0	N/A
	G0/0/1	2001:db 8:5: :1	/64	N/D
	S0/1/0	10.10.3.2	255.255.255.252	N/A
		2001:db 8:3: :2	/126	No corresponde
PC-1	NIC	10.10.1.10	255.255.255.0	10.10.1.1
Portátil A	NIC	10.10.1.20	255.255.255.0	10.10.1.1
PC-2	NIC	2001:db8:1::10	/64	fe80::1
PC-3	NIC	2001:db8:1::20	/64	fe80::1
PC-4	NIC	10.10.5.10	255.255.255.0	10.10.5.1
Servidor 1	NIC	10.10.5.20	255.255.255.0	10.10.5.1
Portátil B	NIC	2001:db 8:5: :10	/64	fe80::1
Portátil C	NIC	2001:db 8:5: :20	/64	fe80::1
Servidor corporativo	NIC	203.0.113.100	255.255.255.0	203.0.113.1
		2001:db8:acad: :100	/64	fe80::1



Objetivos

En esta actividad de Packet Tracer, utilizará ICMP para probar la conectividad de la red y localizar problemas de red. También corregirá problemas de configuración simples y restaurará la conectividad a la red.

- Use ICMP para localizar problemas de conectividad.
- Configure los dispositivos de red para corregir problemas de conectividad.

Aspectos básicos

Los clientes se han quejado de que no pueden llegar a algunos recursos de red. Se le ha pedido que pruebe la conectividad en la red. Utilice ICMP para averiguar qué recursos son inaccesibles y las ubicaciones desde las que no se puede llegar a ellos. A continuación, utilice el seguimiento para localizar el punto en el que se interrumpe la conectividad de red. Finalmente, corrige los errores que encuentra para restaurar la conectividad a la red.

Instrucciones

Todos los hosts deben tener conectividad con todos los demás hosts y con el servidor corporativo.

- Espere hasta que todas las luces de enlace estén verdes.
- Seleccione un host y utilice el ping ICMP para determinar qué hosts son accesibles desde ese host.
- Si se encuentra que un host no es accesible, utilice el seguimiento ICMP para localizar la ubicación general de los errores de red.
- Localice los errores específicos y corrija.

12.3.2 ¿Qué Aprendí en este Módulo?

Mensajes ICMP

Aunque IP es sólo un protocolo de mayor esfuerzo, el conjunto TCP/IP proporciona mensajes de error y mensajes informativos cuando se comunica con otro dispositivo IP. Estos mensajes se envían mediante los servicios de ICMP. El objetivo de estos mensajes es proporcionar

respuestas acerca de temas relacionados con el procesamiento de paquetes IP en determinadas condiciones, no es hacer que IP sea confiable. El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional.

Se puede utilizar un mensaje de eco ICMP para probar la accesibilidad de un host en una red IP. El host local envía una solicitud de eco ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco.

Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje ICMP de destino inalcanzable para notificar al origen que el destino o el servicio son inalcanzables. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete.

Los enrutadores utilizan los mensajes de Tiempo Superado de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo de Tiempo de Duración (TTL) del paquete se disminuyó a 0. Si un router recibe un paquete y disminuye el campo TTL en el paquete IPV4 a cero, descarta el paquete y envía un mensaje de tiempo superado al host de origen.

ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. Los mensajes informativos y de error que se encuentran en ICMPv6 son muy similares a los mensajes de control y de error que implementa ICMPv4. Sin embargo, ICMPv6 incluye cuatro nuevos protocolos como parte de ND o NDP, como se muestra a continuación:

- Mensaje de RS
- Mensaje de RA
- Mensaje de NS
- Mensaje de NA

Pruebas de ping y traceroute

Para probar la conectividad con otro host de una red, se envía una solicitud de eco a la dirección de host mediante el comando **ping**. Si el host en la dirección especificada recibe la solicitud de eco, responde con una respuesta de eco. A medida que se recibe cada respuesta de eco, el comando ping proporciona comentarios acerca del tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta. Esto puede ser una medida del rendimiento de la red. El comando ping tiene un valor de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro del tiempo de espera, el comando ping proporciona un mensaje que indica que no se recibió una respuesta.

Los tipos de pruebas de conectividad que se realizan con ping son los siguientes:

- **Hacer ping a loopback local** - El ping se puede usar para probar la configuración interna de IPv4 o IPv6 en el host local. Para realizar esta prueba, se debe hacer ping a la dirección de loopback local.
- **Hacer ping a la puerta de enlace predeterminada** - Esto generalmente se hace haciendo ping a la dirección IP de la puerta de enlace predeterminada del host. Un ping exitoso a la puerta de enlace predeterminada indica que el host y la interfaz del enrutador que sirven como puerta de enlace predeterminada están operativos en la red local.
- **Hacer ping al host remoto** - Un ping exitoso a través de la red interna confirma la comunicación en la red local, el funcionamiento del enrutador que actúa como puerta de enlace predeterminada y el funcionamiento de todos los demás enrutadores que pueden estar en la ruta entre la red local y la red del anfitrión remoto.

tracert es una utilidad que genera una lista de saltos que se alcanzaron con éxito a lo largo de la ruta. Esta lista puede proporcionar información importante sobre la verificación y la solución de problemas. Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en la ruta entre los hosts. Si los datos fallan en algún salto a lo largo del camino, la dirección del último router que respondió al rastreo puede indicar dónde se encuentra el problema o las restricciones de seguridad.

El tiempo de ida y vuelta es el tiempo que tarda un paquete en llegar al host remoto y que la respuesta del host regrese. Se utiliza un asterisco (*) para indicar un paquete perdido o sin respuesta. Traceroute utiliza una función del campo TTL en IPv4 y el campo Límite de Salto en IPv6 en los encabezados de Capa 3, junto con el mensaje de ICMP Tiempo Excedido.

12.3.3 Webster - Preguntas de Reflexión

No tiene mucho sentido configurar una red si no la prueba para asegurarse de que funciona correctamente. Diego debe asegurarse de que su red funcione y de que se conecte a la red en la sede central y a Internet. Este último módulo del curso Dispositivos de red y configuración inicial proporcionó algunas de las herramientas de solución de problemas más comunes utilizadas por los administradores de redes en todo el mundo. Incluso puede utilizar estas herramientas en su red doméstica. ¡Pruébelo y vea!

12.3.4 Prueba de ICMP

Un técnico utiliza el comando **ping 127.0.0.1**. ¿Qué está probando el técnico?

la pila TCP/IP en un host de red ☺←
conectividad entre dos dispositivos Cisco adyacentes
conectividad entre un PC y la puerta de enlace (gateway) predeterminada
conectividad entre dos computadoras en la misma red
conectividad física de un PC determinado y de la red

¿Qué comando se puede usar para probar la conectividad entre dos dispositivos mediante mensajes de solicitud de eco y respuesta de eco?

netstat	ipconfig
ICMP	ping ☺←

¿Qué contenido de campo utiliza ICMPv6 para determinar que un paquete ha caducado?

Campo TTL	Campo CRC
Campo Limite de Salto ☺←	Campo tiempo excedido

¿Cuál protocolo Proporciona comentarios desde un host de destino a un host de origen con respecto a los errores en la entrega de paquetes?

ARP	BOOTP
DNS	ICMP ☺←

¿Qué mecanismo utiliza un router para evitar que un paquete IPv4 recibido viaje interminablemente en una red?

Comprueba el valor del campo TTL y, si es 0, descarta el paquete y envía un mensaje Destination Unreachable al host de origen.
Comprueba el valor del campo TTL y, si es 100, descarta el paquete y envía un mensaje Destination Unreachable al host de origen.
Reduce el valor del campo TTL en 1 y si el resultado es 0, descarta el paquete y envía un mensaje de Tiempo excedido al host de origen. ☺←
Incrementa el valor del campo TTL en 1 y si el resultado es 100, descarta el paquete y envía un mensaje de problema de parámetro al host de origen.

¿Cuál protocolo utiliza el comando **ping** para probar la conectividad entre los hosts de la red?

ARP	DHCP
TCP	ICMP ☺←

Un usuario está ejecutando el comando **tracert** a un dispositivo remoto. ¿En qué momento dejaría de reenviar el paquete un router que se encuentra en la ruta hacia el dispositivo de destino?

Cuando el router recibe un mensaje de ICMP de tiempo superado
Cuando el valor de RTT llega a cero
Cuando el host responde con un mensaje de respuesta de eco ICMP
Cuando el valor en el campo TTL llega a cero ☺←
Cuando los valores de los mensajes de solicitud de eco y de respuesta de eco llegan a cero

¿Qué protocolo utiliza el comando traceroute para enviar y recibir solicitudes y respuestas de eco?

SNMP	ICMP ☺←
TELNET	TCP

¿Qué mensaje envía un host para comprobar la singularidad de una dirección IPv6 antes de usar esa dirección?

solicitud de vecino ☺←	solicitud de ARP
solicitud de eco	solicitud de router

¿Qué tipo de mensaje ICMPv6 proporciona información de direccionamiento de red a los hosts que utilizan SLAAC?

Solicitud de vecino	Oferta (o anuncio) de router ☺←
Oferta (o anuncio) de vecino	solicitud de router

Un usuario ejecuta un traceroute a través de IPv6. ¿En qué momento dejaría de reenviar el paquete un router que se encuentra en la ruta hacia el dispositivo de destino?

cuando el valor del campo Límite de saltos alcanza 255
cuando el valor del campo Límite de saltos alcanza cero ☺←
cuando el router recibe un mensaje de ICMP de tiempo excedido
cuando el host responde con un mensaje de respuesta de eco ICMP

Un usuario emite un comando **ping 198.51.100.25** y recibe una respuesta que incluye un código de **2**. ¿Qué representa este código?

puerto inalcanzable	host fuera de alcance
protocolo inalcanzable ☺←	red inalcanzable

Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 10 – 12

Bienvenido al Examen de Control de Dispositivos de Red y Configuración Inicial Módulos 10 - 12.
Esta evaluación cubre los conceptos básicos y las habilidades presentadas en los Módulos 10 al 12 del curso Dispositivos de Red y Configuración Inicial.
Hay 21 preguntas en total. Debe alcanzar el 70% para aprobar este examen.
Tiene intentos ilimitados para aprobar el examen. Se proporcionan comentarios para dirigirlo a áreas que pueden requerir atención adicional.
El contenido de Cisco Networking Academy está protegido por leyes de derechos de autor y está prohibido publicar, distribuir o compartir el contenido de este examen sin autorización.
© 2022, Cisco Systems, Inc.
¿Qué comando de switch usaría un administrador de red para determinar si hay errores de medios o encapsulamiento en una interfaz?

show arp	show line
show ip interface	show interfaces ☺←

Explicación: El comando ***show interfaces*** es útil para detectar errores de medios, para ver si los paquetes se envían y reciben, y para determinar si se han producido runts, gigantes, CRC, reinicios de interfaz u otros errores. El comando ***show ip interface*** es útil para ver si la interfaz está «activa». La salida del comando ***show line*** muestra parámetros para las líneas activas que están en uso, como la línea vty utilizada para Telnet. El comando ***show arp*** muestra el contenido de la tabla del Protocolo de Resolución de Direcciones (ARP).

¿Cuál modo de Cisco IOS muestra un indicador de **Router#**?

modo de configuración inicial	modo EXEC del usuario
modo EXEC privilegiado ☺←	modo de configuración global

¿Qué significa la letra C junto a una entrada en la salida del comando **show ip route**?

Identifica una red que se aprende a través de OSPF.	Identifica una red que es una ruta estática.
Identifica una red que se aprende a través de EIGRP.	Identifica una red que está conectada directamente al router. ☺←

Explique: En una tabla de enrutamiento, la etiqueta C identifica una red que está conectada directamente a una interfaz del dispositivo. Esta entrada se agrega a la tabla de enrutamiento cuando se configura una interfaz con una dirección IP y se activa.

Observe la ilustración. ¿Qué elemento de sintaxis de IOS es la expresión **MainOffice**?

```
Switch(config)# hostname MainOffice
```

un argumento ☺←	un subcomando
un comando	una palabra clave

Explique: Un ***argumento*** de un comando de la CLI generalmente no es una palabra predefinida, sino que es un valor definido por el usuario. Las palabras clave, sin embargo, describen parámetros específicos de un comando que son palabras predefinidas que el intérprete de comandos conoce.

Observe la ilustración. Un administrador está intentando configurar el conmutador, pero recibe el mensaje de error que se muestra en la imagen. ¿Cuál es el problema?

```
Switch1> config t
               ^
% Invalid input detected at '^' marker.
```

El administrador ya está en modo de configuración global.
Se debe utilizar todo el comando, configure terminal.
El administrador debe conectarse a través del puerto de la consola para acceder al modo de configuración global.
El administrador primero debe ingresar al modo EXEC privilegiado antes de emitir el comando. ☺←

Explique: Para ingresar al modo de configuración global, se debe introducir el comando ***configure terminal*** o una versión abreviada, como ***config t*** , desde el modo EXEC privilegiado. En esta situación, el administrador está en el modo EXEC del usuario, según lo indica el símbolo **>** después del nombre de host. El administrador debe utilizar el comando ***enable*** para pasar al modo EXEC privilegiado antes de introducir el comando ***configure terminal*** .

Un administrador utiliza la combinación de teclas Ctrl-Shift-6 en un conmutador después de emitir el comando **ping**. ¿Cuál es el propósito de utilizar estas teclas?

para reiniciar el proceso de ping	para salir a un modo de configuración diferente
para interrumpir el proceso de ping ☺←	para permitir al usuario completar el comando

Explique: Para interrumpir un proceso del IOS, como ping o traceroute, el usuario introduce la combinación de teclas ***Ctrl-Mayús-6***. La tecla de tabulación completa el resto de los parámetros o de los argumentos de un comando. Para salir del modo de configuración y pasar al modo privilegiado, pulse las teclas Ctrl-Z. Ctrl-R vuelve a mostrar la línea que se acaba de escribir, de modo que resulta más fácil para el usuario presionar la tecla Entrar y volver a emitir el comando ping.

Para ahorrar tiempo, los comandos de IOS pueden ingresarse parcialmente y luego completarse tecleando qué combinación de teclas o teclas.

Ctrl-P	Flecha derecha
Flecha arriba	Flecha hacia abajo
Tabulación ☺←	Ctrl-N

Las contraseñas se pueden usar para restringir el acceso a Cisco IOS o a partes de este. Seleccione los modos e interfaces que pueden protegerse con contraseñas. (Elija tres opciones).

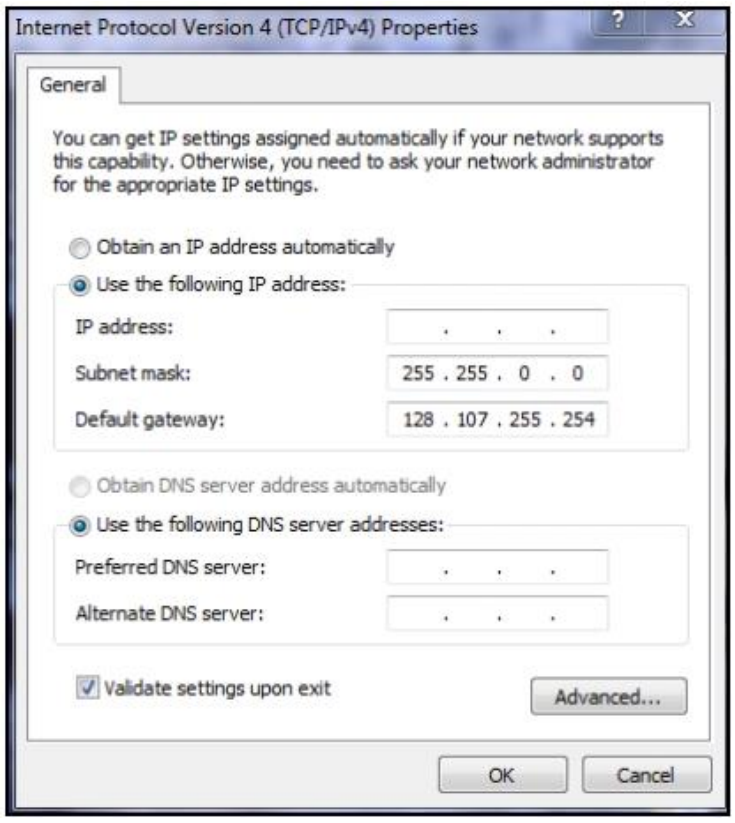
Interfaz VTY ☺←	modo EXEC privilegiado ☺←
Interfaz de la consola ☺←	Modo de arranque IOS
Modo de configuración del enrutador	Interfaz Ethernet

Explique: El acceso a las interfaces de consola y VTY se puede restringir utilizando contraseñas. La administración fuera de banda del router se puede restringir en los modos EXEC del usuario y EXEC privilegiado.

¿Cuál de las siguientes interfaces es la SVI predeterminada en un conmutador Cisco?

VLAN 1 ☺←	GigabitEthernet 0/1
VLAN 99	FastEthernet 0/1

Observe la ilustración. Un técnico en redes está asignando estáticamente una dirección IP a una PC. La puerta de enlace predeterminada es correcta. ¿Cuál sería una dirección IP válida para asignar al host?



128.107.255.254	128.107.255.1 ☺←
128.108.100.10	128.106.10.100

Al configurar SSH en un enrutador para implementar una gestión segura de red, un ingeniero de red ha emitido los comandos **login local** y **transport input ssh** line vty. ¿Qué tres acciones de configuración adicionales se deben realizar para completar la configuración SSH? (Elija tres opciones).

- Establecer los niveles de privilegios de usuario.
- Configurar acceso a la CLI basado en funciones
- Configurar el nombre de dominio IP correcto. ☺←
- Crear un base de datos de nombre de usuario y de contraseñas locales. ☺←
- Habilitar SSH manualmente después de generar las claves RSA.
- Generar las claves RSA asimétricas. ☺←

Explique: SSH se habilita automáticamente después de generar las claves RSA. Establecer niveles de privilegios de usuario y configurar el acceso a la CLI basado en roles son buenas prácticas de seguridad, pero no son un requisito para implementar SSH.

Una el tipo de contraseña en un dispositivo Cisco con su función.

Contraseña enable	✓ Limita el acceso al modo EXEC privilegiado
Contraseña de consola	✓ Limita el acceso al dispositivo a traves de una conexión SSH
Habilitar secreto	✓ Limita el acceso al dispositivo a traves de una conexion fuera de banda
Contraseña vty	✓ Cifra la contraseña y restringe en acceso al modo EXEC privilegiado

Una el comando con el modo de dispositivo en el que se introduce.

login	✓ R1(config)#
service password-encryption	✓ R1>
copy running-config startup-config	✓ R1#
enable	✓ R1(config-line)#
ip address 192.168.4.4 255.255.255.0	✓ R1(config-if)#

Explique: El comando **enable** se introduce en el modo R1>. El comando **login** se introduce en el modo R1(config-line)#. El comando **copy running-config startup-config** se introduce en el modo R1#. El comando **ip address 192.168.4.4 255.255.255.0** se introduce en el modo R1(config-if)#. El comando **service password-encryption** se introduce en el modo de configuración global.

Un administrador de red establece una conexión a un switch a través de SSH. ¿Qué característica describe de forma única la conexión SSH?

- acceso remoto a un switch donde los datos se cifran durante la sesión ☺←
- acceso directo al switch mediante el uso de un programa de emulación de terminal
- acceso remoto al switch mediante el uso de una conexión telefónica
- acceso fuera de banda a un switch mediante el uso de un terminal virtual con autenticación de contraseña
- acceso in situ a un switch mediante el uso de un PC conectado directamente y un cable de consola

Explique: SSH proporciona un inicio de sesión remoto seguro a través de una interfaz virtual. SSH proporciona una autenticación de contraseña más segura que Telnet. SSH también cifra los datos durante la sesión.

Un usuario emite un comando ping **198.51.100.5** y recibe una respuesta que incluye un código de **3**. ¿Qué representa este código?

puerto inalcanzable ☺←	protocolo inalcanzable
red inalcanzable	host fuera de alcance

Explique: Cuando un host o una puerta de enlace recibe un paquete que no puede entregar, puede usar un mensaje de destino inalcanzable de ICMP para notificar al origen que el destino o el servicio no son accesibles. El mensaje incluirá un código que indica por qué no se pudo entregar el paquete. Estos son algunos de los códigos de destino inalcanzable para ICMPv4:
0: red inalcanzable
1: host inalcanzable
2: protocolo inalcanzable
3: puerto inalcanzable

Un usuario llama para reportar que una computadora no puede acceder a internet. El técnico de red pide al usuario que ejecute el comando **ping 127.0.0.1** en una ventana de Símbolo del sistema (Command Prompt). El usuario informa que el resultado es cuatro respuestas positivas. ¿Qué conclusión se puede extraer basándose en esta prueba de conectividad?

- La dirección IP obtenida del servidor DHCP es correcta.
- La implementación TCP/IP es funcional. ☺←
- La computadora puede acceder a internet. Sin embargo, es posible que el web browser (navegador web) no funcione.
- La computadora puede acceder a la red. El problema existe más allá de la red local.

Explique: El **ping 127.0.0.1** comando se utiliza para comprobar que la pila TCP/IP es funcional. Esto verifica que el stack de protocolos funcione correctamente desde la capa de red hasta la capa física, sin enviar una señal en los medios. Es decir, esta prueba no va más allá de la PC en sí. Por ejemplo, no detecta si un cable está conectado a la PC o no.

¿Qué mensaje ICMPv6 se envía cuando el campo de límite de saltos IPv6 de un paquete se reduce a cero y el paquete no se puede reenviar?

red inalcanzable	Tiempo excedido ☺←
Puerto inalcanzable	Protocolo inalcanzable

Explique: ICMPv6 utiliza el campo de límite de saltos en el encabezado del paquete IPv6 para determinar si el paquete ha caducado. Si el campo límite de salto ha alcanzado cero, un router enviará un mensaje de tiempo excedido hacia el origen indicando que el router no puede reenviar el paquete.

¿Qué utilidad utiliza el Protocolo de mensajería de control de Internet?

NTP	RIP	DNS	ping ☺←

¿Qué mensaje ICMP utiliza la utilidad traceroute durante el proceso de encontrar la ruta entre dos hosts finales?

Redireccionamiento	Tiempo superado ☺←	Destino inalcanzable	ping

Explique: Traceroute incrementa progresivamente el campo TTL (IPv4) o límite de salto (IPv6) (1, 2, 3, 4…) para enviar secuencia de comandos ping. Cuando un router detecta que el TTL o límite de salto es 0, descartará el paquete y enviará un mensaje de tiempo excedido al origen del traceroute. El mensaje devuelto contiene la dirección IP del enrutador que descartó el paquete. Por lo tanto, la utilidad traceroute aprende la dirección del enrutador. Este proceso continúa y proporciona la traza con la dirección de cada salto (enrutador) a medida que los paquetes continúan viajando a través de enrutadores para llegar al destino.

¿Qué comando puede utilizarse para verificar la conectividad entre dos dispositivos host?

nslookup	netstat	ipconfig	ping ☺←

Abra la actividad de PT. Realice las tareas en las instrucciones de la actividad y luego responda la pregunta.

Abra el símbolo del sistema en PC2 y use el comando **ipv6config** para anotar la dirección IPv6 de PC2. Abra el símbolo del sistema en PC1 y trace la ruta a PC2. ¿Cuáles son las tres direcciones IPv6 que se muestran cuando se traza la ruta de PC1 a PC2? (Elija tres.)

- ✓ 2001:DB8:1:2::1
- ✓ 2001:DB8:1:1::1
- 2001:DB8:1:2::2
- ✓ 2001:DB8:1:3::2
- 2001:DB8:1:3::1
- 2001:DB8:1:4::1
- 2001:DB8:1:1::A

Examen Final de Dispositivos de Red y Configuración Inicial

Bienvenido al Examen Final de Dispositivos de Red y Configuración Inicial.
Esta evaluación cubre los conceptos y las habilidades fundamentales presentados en el curso Dispositivos de Red y Configuración Inicial.
Hay 30 preguntas en total. Debe alcanzar el 70% para aprobar este examen.
Tiene intentos ilimitados para aprobar el examen. Se proporcionan comentarios para dirigirlo a áreas que pueden requerir atención adicional.
El contenido de Cisco Networking Academy está protegido por leyes de derechos de autor y está prohibido publicar, distribuir o compartir el contenido de este examen sin autorización.
© 2022, Cisco Systems, Inc.

Una la definición con el tipo de nube.

Compuesto por dos o más infraestructuras de nube distintas unidas por tecnología	✓ Nube comunitaria
Servicios puestos a disposición de la población en general	✓ Nube pública
Destinado a una organización o entidad específica, como el gobierno	✓ Nube híbrida
Destinado al uso exclusivo de múltiples organizaciones con necesidades funcionales compartidas	✓ Nube privada

Explique: Los servicios de nube pública están a disposición de la población en general. Los servicios de nube privada están destinados a una organización o una entidad específica. Una nube personalizada se diseña para satisfacer las necesidades de un sector específico. Una nube híbrida consta de dos o más nubes que están conectadas a través de una sola arquitectura.

¿Cuál es un ejemplo de computación en la nube?

- Un estilo arquitectónico de la red informática mundial.
- Una interacción continua entre las personas, los procesos, los datos y las cosas.
- Una infraestructura de red que abarca un área geográfica extensa.
- Un servicio que ofrece acceso a pedido a los recursos compartidos. ☺←

¿Cuáles dos situaciones beneficiarían más al usuario al agregar calidad de servicio (QoS) a la red? (Elija dos opciones).

- Un estudiante se comunica por Skype con un amigo en otro país. ☺←
- Los estudiantes están viendo una conferencia desde un sitio de YouTube. ☺←
- Los estudiantes actualizan información sobre sus actividades deportivas en la página de Facebook de la clase.
- Un estudiante está enviando correos electrónicos a un amigo.

Explique: Los datos de voz y video deben transmitirse en un flujo continuo. Si los paquetes se retrasan, la calidad de audio y video será deficiente, a veces incluso no utilizable. QoS puede dar alta prioridad a los datos de voz y video durante la transmisión de datos para que se envíen primero antes que otros tipos de tráfico, como correo electrónico, navegación web y actualización de la página web.

Un empleado de una gran corporación inicia sesión de forma remota en la empresa utilizando el nombre de usuario y la contraseña apropiados. El empleado está asistiendo a una importante videoconferencia con un cliente sobre una gran venta. Es importante que la calidad del video sea excelente durante la reunión. El empleado no sabe que después de un inicio de sesión exitoso, la conexión con el ISP de la empresa falló. La conexión secundaria, sin embargo, se activa en cuestión de segundos. La interrupción no fue notada por el empleado u otros empleados. ¿Qué tres características de red se describen en este escenario? (Elija tres opciones).

Seguridad ☺←	QoS ☺←
Escalabilidad	Tolerancia a fallas ☺←
Redes por línea eléctrica	Integridad

Explique: Los nombres de usuario y las contraseñas se relacionan con la seguridad de la red. Vídeo de buena calidad, para soportar videoconferencias, se refiere a priorizar el tráfico de vídeo con calidad de servicio (QoS). El hecho de que una conexión a un ISP falle y luego se restableció, pero pasó desapercibido por los empleados se relaciona con el diseño tolerante a fallos de la red.

¿Cuál es la diferencia clave entre un hipervisor de tipo 1 y un hipervisor de tipo 2?

- Un hipervisor tipo 1 admite toda la virtualización del SO del servidor y un hipervisor tipo 2 admite la virtualización de Linux y Mac.
- Un hipervisor tipo 1 se ejecuta en sistemas especializados y un hipervisor tipo 2 en computadoras de escritorio.
- Un hipervisor tipo 1 admite virtualizaciones de servidor y un hipervisor tipo 2 solo admite virtualización de estación de trabajo.
- Un hipervisor de tipo 1 se ejecuta directamente en el hardware del sistema y un hipervisor de tipo 2 requiere un SO de host para ejecutarse ☺←

¿Cuáles tres afirmaciones describen las funciones del modelo de diseño de red jerárquico de Cisco? (Elija tres opciones).

- La capa de acceso proporciona un medio para conectar dispositivos finales a la red. ☺←
- El objetivo de la capa de núcleo es maximizar el rendimiento. ☺←
- La capa de núcleo generalmente emplea una topología en estrella.
- La capa de distribución distribuye el tráfico de red directamente a los usuarios finales.
- El resumen de ruta no es necesario en las capas de núcleo y distribución.
- La capa de distribución es responsable de filtrar el tráfico y aislar las fallas del núcleo. ☺←

Un centro de datos ha actualizado recientemente un servidor físico para alojar varios sistemas operativos en un solo CPU. El centro de datos ahora puede proporcionar a cada cliente un servidor web independiente sin tener que asignar un servidor discreto real para cada cliente. ¿Cuál es la tendencia de la red que implementa el centro de datos en esta situación?

Virtualización ☺←	Colaboración en línea
Mantener la integridad de la comunicación	BYOD

Explique: La tecnología de virtualización puede ejecutar varios sistemas operativos diferentes en paralelo en una sola CPU.

¿Qué tres campos del encabezado IPv4 no están en un encabezado IPv6? (Elija tres opciones).

Señalización ☺←	TTL
Identificación ☺←	Protocolo
Desplazamiento de fragmentos ☺←	Versión

Explique: A diferencia de IPv4, los routers IPv6 no realizan fragmentación. Por lo tanto, los tres campos relacionados con la fragmentación en el encabezado IPv4 se quitan y no están presentes de igual manera en el encabezado IPv6. Estos tres campos son desplazamiento de fragmentos, señalización e identificación. IPv6 sí admite la fragmentación de paquetes del host mediante el uso de encabezados de extensión, que no son parte del encabezado IPv6.

Haga coincidir los nombres de campo con el encabezado IP donde se encontrarán.

Señaladores
Encabezado IP v4
Clase de tráfico
Encabezado IP v6
Longitud Total
Encabezado IP v4
Etiqueta de flujo
Encabezado IP v6

¿Cuál es el propósito de la dirección MAC que se agrega a un mensaje de correo electrónico que se envía de un maestro a un alumno?

- Identifica la aplicación de red TCP/ P a la que se puede enviar la respuesta.
- Identifica la computadora en la LAN. ☺←
- Identifica la computadora en Internet.
- Identifica la red a la que pertenece el equipo emisor.

¿Cuáles dos afirmaciones son correctas en una comparación de encabezados de paquetes IPv4 e IPv6? (Elija dos opciones).

- El nombre del campo de suma de verificación de encabezado de IPv4 se mantiene en IPv6.
- El campo Versión de IPv4 no se mantiene en IPv6.
- El campo Tiempo de vida de IPv4 se reemplazó por el campo Límite de saltos de IPv6. ☺←
- El campo Dirección de destino es nuevo en IPv6.
- El nombre del campo de dirección de origen de IPv4 se mantiene en IPv6. ☺←

¿Cuál de las siguientes es la representación decimal punteada de la dirección IPv4

11001011.00000000.01110001.11010011?

198.51.100.201	209.165.201.223
203.0.113.211 ☺←	192.0.2.199

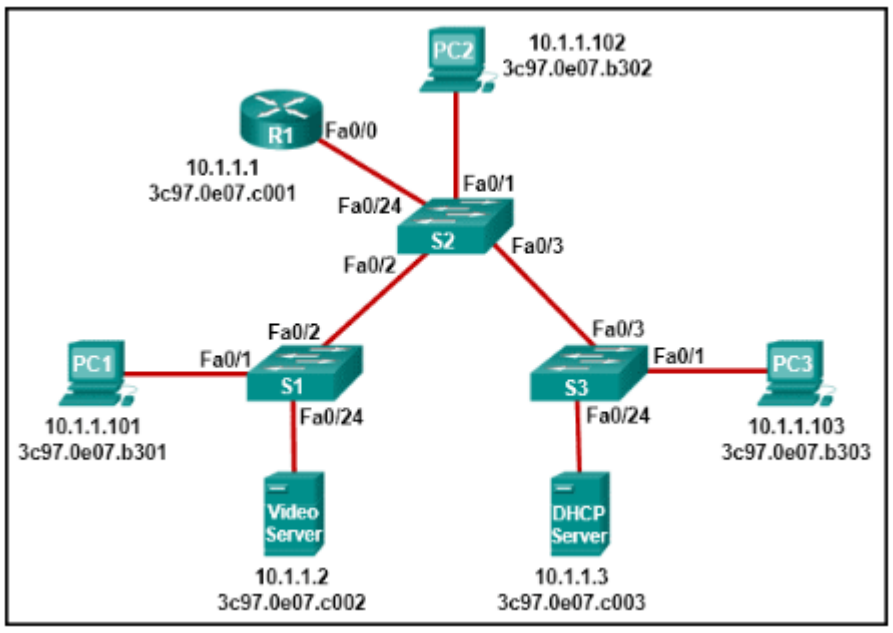
Haga coincidir el campo del encabezado del paquete IPv6 con la descripción.

Limite de Saltos	Campo de 8 bits que es equivalente al campo de Servicios Diferenciados (DS) de IPv4.
Clase de Tráfico	Campo de 8 bits que indica el tipo de carga de datos.
Longitud de la Carga Útil	Campo de 20 bits que mantiene el mismo flujo de paquete a través de los enrutadores y conmutadores para garantizar que el paquete llegue en el mismo orden.
Siguiente Encabezado	Campo de 16 bits que estipula la longitud de la porción de datos del paquete IPv6.
Etiqueta de Flujo	Campo de 8 bits que se decrementa en uno por cada enrutador que reenvía el paquete.

¿Cuáles dos elementos utiliza un dispositivo host al realizar una operación de AND para determinar si una dirección de destino está en la misma red local? (Elija dos opciones).

- Dirección IP de destino ☺←
- máscara de subred ☺←
- número de red
- Dirección MAC de origen
- Dirección MAC de destino

Observe la ilustración. La PC1 envía una trama con la dirección MAC de destino 3c97.0e07.a1b2. El Switch S1 busca la dirección MAC de destino en su tabla CAM pero la dirección no está allí. ¿Qué hará el switch?



Reenviará la trama a todos los puertos excepto Fa0/1. ☺←

El switch descartará la trama.

Reenviará la trama desde el puerto Fa0/2 hacia el router.

Agregará la dirección MAC de destino a la tabla MAC.

Enviará un mensaje de destino inalcanzable a la PC1.

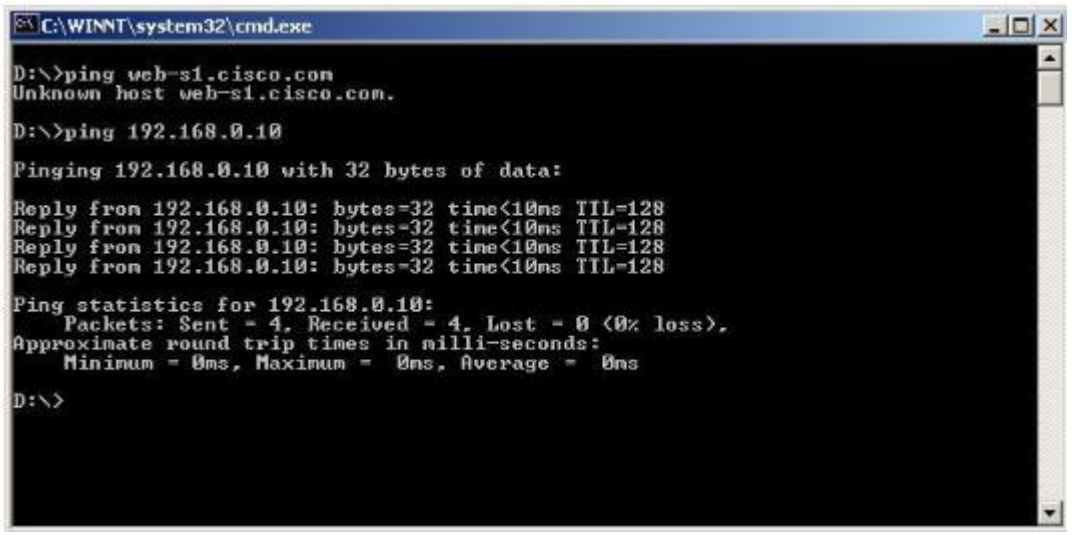
Unir cada tipo de mensaje de DHCP con la descripción correspondiente.

DHCPDISCOVER	✓ un cliente que inicia un mensaje para encontrar un servidor DHCP
DHCPACK	✓ un servidor DHCP que responde a la solicitud inicial de un cliente
DHCPREQUEST	✓ el cliente aceptando la dirección IP proporcionada por el servidor DHCP
DHCPOFFER	✓ el servidor DHCP que confirma que se ha aceptado la concesión de la dirección

Asocie las características con la categoría del protocolo.

Tamaño de ventana	
TCP	✓
Sin conexión	
UDP	✓
Suma de comprobación	
UDP y TCP	✓

Observe la ilustración. Un diseñador web llama para informar que no se puede conectar con el servidor web web-s1.cisco.com a través de un navegador web. El técnico usa las utilidades de la línea de comando para verificar el problema y para comenzar con el proceso de solución de problemas. ¿Cuáles son los dos hechos se pueden determinar sobre el problema? (Elija dos opciones).



- Un enrutador no está funcionando entre el host de origen y el servidor web-s1.cisco.com.
- Está desactivada la puerta de enlace predeterminada entre el host de origen y el servidor en 192.168.0.10.
- El DNS no puede resolver la dirección IP para el servidor web-s1.cisco.com. ☺←
- Existe un problema con el software del servidor Web en web-s1.cisco.com.
- Se puede alcanzar el servidor Web en 192.168.0.10 desde el host de origen. ☺←

Una red doméstica tiene tanto conectividad cableada e inalámbrica. Desde una computadora portátil, el usuario emite un ping a la impresora inalámbrica ubicada en otra sala. Las primeras dos solicitudes de eco fallan, pero las dos últimas tienen éxito. Los pings adicionales son exitosos. ¿Por qué fallan las dos primeras solicitudes de eco?

- La impresora inalámbrica debe estar activada y eso lleva tiempo.
- La computadora debe utilizar ARP para obtener la dirección MAC de la impresora y este proceso lleva tiempo. ☺←
- La distancia entre la computadora y la impresora causa demora en los primeros dos pings
- La computadora y la impresora deben conectarse primero a la red inalámbrica y ese proceso lleva tiempo.

¿Qué afirmación es verdadera con respecto al proceso del cliente UDP durante una sesión con un servidor?

- Los servidores de aplicaciones deben utilizar números de puerto superiores a 1024 para admitir UDP.
- Se realiza un protocolo de enlace de tres vías antes de que comience la transmisión de datos.
- Se debe establecer una sesión para poder intercambiar datagramas.
- Los datagramas que llegan en un orden diferente al que se enviaron no se colocan en orden. ☺←

Explique: Debido a que no hay números de secuencia en los segmentos UDP, no hay posibilidad de organizar los datagramas en el orden correcto. Las sesiones y el protocolo de enlace de tres vías están relacionados con las comunicaciones TCP. Los servidores UDP pueden usar números de puerto registrados o no registrados para escuchar a los clientes.

¿Cuáles son dos posibles problemas de red que pueden resultar de la operación de ARP? (Elija dos opciones).

- Un gran número de transmisiones de solicitud de ARP puede hacer que la tabla de direcciones MAC del host se desborde y evitar que el host se comunique en la red.
- Los atacantes de red pueden manipular la asignación de direcciones MAC y direcciones IP en mensajes ARP con la intención de interceptar el tráfico de red. ☺←
- La configuración manual de asociaciones de ARP estáticas podría facilitar el envenenamiento por ARP o la suplantación de direcciones MAC.
- En redes grandes con poco ancho de banda, varias transmisiones ARP pueden causar demoras en la comunicación de datos. ☺←
- Varias respuestas ARP dan como resultado que la tabla de direcciones MAC del switch contenga entradas que coincidan con las direcciones MAC de los hosts que están conectados al puerto de switch correspondiente.

Explique: Un gran número de mensajes de broadcast de ARP podría generar retrasos momentáneos en las comunicaciones de datos. Los atacantes de la red podrían manipular las asignaciones de direcciones MAC e IP en mensajes ARP con el objetivo de interceptar el tráfico de la red. Las solicitudes de ARP y las respuestas hacen que se creen entradas en la tabla ARP, no en la tabla de direcciones MAC. Los desbordamientos de la tabla ARP son muy poco probables. Configurar manualmente asociaciones ARP estáticas es una manera de impedir el

envenenamiento ARP y la suplantación de direcciones MAC, no de facilitarlos. Las diversas respuestas ARP, cuyo resultado es la tabla de direcciones MAC del switch que contiene entradas que coinciden con las direcciones MAC de los nodos conectados y están asociadas al puerto del switch pertinente, son necesarias para las operaciones normales de reenvío de tramas del switch. No se trata de un problema de red causado por ARP.

Haga coincidir el señalador TCP con el paso correcto en la secuencia de establecimiento de la sesión.

Paso 1	ACK
Paso 3	SYN
Paso 2	SYN + ACK

¿Cuáles tres pasos de configuración se deben realizar para implementar el acceso SSH a un router? (Elija tres opciones).

un nombre de dominio IP ☺←	una contraseña en la línea de consola
una cuenta de usuario ☺←	un nombre de host único ☺←
una contraseña cifrada	una contraseña de modo de activación

Explique: Para implementar SSH en un router es necesario realizar los siguientes pasos:

- Configure un nombre de host único.
- Configurar el nombre de dominio de la red.
- Configurar una cuenta de usuario para utilizar la base de datos AAA o local para la autenticación.
- Generar claves RSA.
- Habilitar sesiones SSH VTY.

Una el indicador del enrutador con la tarea de configuración.

RouterA(config)#	Configurar lineas vty
RouterA(config-if)#	Configurar una interfaz WAN
RouterA(config-line)#	Entrar en el modo de configuración
RouterA#	Agregue una contraseña requerida para acceder al modo EXEC privilegiado

El comando de configuración global **ip default-gateway 172.16.100.1** se aplica a un switch. ¿Cuál es el efecto de este comando?

El switch tendrá una interfaz de administración con la dirección 172.16.100.1.
El switch se puede administrar de forma remota desde un host en otra red. ☺←
El switch está limitado a enviar y recibir tramas desde y hacia la puerta de enlace 172.16.100.1.
El switch puede comunicarse con otros hosts de la red 172.16.100.0.

Explique: Normalmente, una dirección de puerta de enlace predeterminada se configura en todos los dispositivos para permitirles comunicarse más allá de su red local. En un switch, esto se logra mediante el comando ip default-gateway ip address.

Al tratar de solucionar un problema de la red, el administrador de red ejecuta el comando **show version** en un enrutador. ¿Qué información se puede encontrar con este comando?

La cantidad de memoria RAM no volátil (NVRAM), DRAM y flash instalada en el enrutador. ☺←
Las diferencias entre la configuración de respaldo y la configuración en ejecución actual.
La versión del protocolo de enrutamiento que se está ejecutando en el enrutador.
El ancho de banda, la encapsulación y las estadísticas de E/S en las interfaces.

¿Qué protocolo utiliza IPv4 e IPv6 para proporcionar mensajes de error?

DHCP	NDP
ICMP ☺←	ARP

Un administrador de red emite el comando Switch# **show running-config** en un conmutador Cisco. ¿Qué término se utiliza para describir la parte "**running-config**" en el comando?

Argumento	Comando
Teclas rápidas	Palabra clave ☺←

¿Cuáles son los tres comandos que se utilizan para configurar el acceso seguro a un enrutador mediante una conexión a la interfaz de consola? (Elija tres opciones).

Login ☺←	password cisco ☺←
line vty 0 4	enable secret cisco
interface fastethernet 0/0	line console 0 ☺←

Explique: Los tres comandos que se necesitan para proteger con contraseña el puerto de consola son los siguientes:
line console 0
password cisco
login
El comando interface fastethernet 0/0 se suele utilizar para acceder al modo de configuración que se utiliza para aplicar parámetros específicos, como la dirección IP, al puerto Fa0/0. El comando line vty 0 4 se utiliza para acceder al modo de configuración para Telnet. Los parámetros 0 y

4 especifican los puertos de 0 a 4 o un máximo de cinco conexiones Telnet simultáneas. El comando enable secret se utiliza para aplicar una contraseña utilizada en el router y acceder al modo privilegiado.

¿Cuál es la diferencia entre los términos palabra clave y argumento en la estructura de un comando IOS?

- Una palabra clave se ingresa con una longitud predefinida. Un argumento puede tener cualquier longitud.
- Una palabra clave siempre aparece directamente después de un comando. Un argumento no.
- Una palabra clave es un parámetro específico. Un argumento no es una variable predefinida. ☺←
- Se requiere una palabra clave para completar un comando. No así un argumento.

FIN DEL CURSO